

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕНО  
ШКНР.00051-01 33 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС  
SIGNAL-COM CLOUD DSS  
Версия 1.0

Руководство программиста

ШКНР.00051-01 33 01  
Листов 88

## **АННОТАЦИЯ**

Настоящий документ содержит описание программного интерфейса программно-аппаратного комплекса Signal-COM Cloud DSS, предназначенного для централизованного дистанционного создания, обслуживания и применения ключей электронной подписи.

## СОДЕРЖАНИЕ

Аннотация .....	2
Содержание .....	3
1. Назначение и условия применения .....	5
1.1. Список сокращений .....	5
1.2. Термины и определения .....	5
2. Характеристика программы .....	7
3. Обращение к программе .....	8
3.1. Базовые структуры и типы данных .....	8
3.1.1. Структура RequestBaseType .....	8
3.1.2. Структура ResponseBaseType .....	8
3.1.3. Структура KeySelectorType .....	9
3.2. Синхронное и асинхронное выполнение операций .....	9
3.3. Интерфейс пользователя .....	10
3.3.1. Метод getCAInfo .....	10
3.3.2. Метод getCertificationRequestTemplateInfo .....	11
3.3.3. Метод generateKeyPair .....	13
3.3.4. Метод generateCertificationRequest .....	15
3.3.5. Метод getKeyEntryInfo .....	17
3.3.6. Метод updateKeyEntryInfo .....	20
3.3.7. Метод deleteKeyEntry .....	21
3.3.8. Метод getTokenInfo .....	21
3.3.9. Метод updateTokenInfo .....	22
3.3.10. Метод sign .....	23
3.3.10.1 Создание ЭП в формате CMS .....	28
3.3.10.2 Создание ЭП в формате CMS с добавлением метки доверенного времени ....	29
3.3.10.3 Добавление метки доверенного времени в CMS подпись .....	29
3.3.10.4 Создание ЭП в формате XMLDSig .....	29
3.3.10.5 Создание ЭП документа в формате PDF .....	30
3.3.10.6 Создание ЭП документа в формате Office Open XML .....	30
3.3.11. Метод verify .....	30
3.3.11.1 Проверка ЭП в формате CMS .....	33
3.3.11.2 Добавление метки доверенного времени к ЭП в формате CMS .....	33
3.3.11.3 Создание усовершенствованной ЭП в формате CMS .....	33
3.3.11.4 Проверка ЭП в формате XMLDSig .....	33
3.3.11.5 Проверка ЭП документа в формате PDF .....	34
3.3.11.6 Проверка ЭП документа в формате Office Open XML .....	34
3.3.11.7 Удаление ЭП из документа в формате PDF .....	34
3.3.12. Метод getUserInfo .....	34
3.3.13. Метод updateUserInfo .....	36
3.3.14. Метод encrypt .....	36
3.3.15. Метод decrypt .....	37
3.3.16. Метод getGroupInfo .....	38
3.4. Интерфейс оператора .....	38
3.4.1. Метод getCAInfo .....	38
3.4.2. Метод getGroupInfo .....	39
3.4.3. Метод getOtpClientInfo .....	40
3.4.4. Метод addCustomer .....	42
3.4.5. Метод getCustomerInfo .....	44
3.4.6. Метод updateCustomerInfo .....	45
3.4.7. Метод deleteCustomer .....	45
3.4.8. Метод getCustomerKeyEntryInfo .....	46
3.4.9. Метод generateCustomerCMC .....	46
3.4.10. Метод updateCustomerKeyEntryInfo .....	47
3.4.11. Метод getCustomerTokenInfo .....	47
3.4.12. Метод updateCustomerTokenInfo .....	48
3.4.13. Метод getUserInfo .....	48
3.4.14. Метод updateUserInfo .....	48
3.4.15. Метод getCustomerObjects .....	49

---

3.4.16.	Метод confirmCustomerInfo .....	50
3.4.17.	Метод getCustomerPSK .....	51
4.	Входные и выходные данные .....	52
5.	Сообщения .....	53
6.	Аутентификация пользователей и получение маркера доступа .....	56
6.1.	Протокол OAuth.....	56
6.1.1.	Получение кода авторизации.....	56
6.1.2.	Получение маркера доступа .....	57
6.1.3.	Подтверждение операции пользователя .....	57
6.1.4.	Обновление маркера доступа .....	59
6.1.5.	Обновление маркера доступа при подтверждении операции пользователя .....	59
6.1.6.	Использование стандартных клиентов OAuth 2.0 .....	59
6.1.7.	Завершение сессии пользователя на сервере идентификации (logout) .....	59
6.2.	Протокол WS-Trust .....	61
6.2.1.	Получение маркера доступа .....	61
6.2.2.	Подтверждение операции пользователя .....	66
Приложение А. Взаимодействие клиента с веб-сервисом идентификации при аутентификации пользователя .....		69
Приложение Б. Взаимодействие клиента с веб-сервисом пользователя и веб-сервисом идентификации при подтверждении операции пользователя .....		71
Приложение В. Примеры запросов .....		75
Литература .....		87

## 1. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

Программно-аппаратный комплекс Signal-COM Cloud DSS (далее Cloud DSS) предназначен для централизованного дистанционного создания, хранения, обслуживания и применения ключей электронной подписи и сертификатов ключей проверки электронной подписи.

Cloud DSS позволяет выполнять операции создания и проверки электронных подписей в форматах CMS, CAdES, PAdES, XMLDSig, Office OpenXML. Дополнительно реализована возможность зашифрования и расшифрования данных в формате CMS.

В Cloud DSS реализован интерфейс взаимодействия с Удостоверяющими центрами, облегчающий пользователям регистрацию и получение сертификатов ключей проверки электронной подписи.

Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам SOAP [1] и REST.

### 1.1. Список сокращений

В настоящем руководстве используются следующие сокращения:

- ПАК – программно-аппаратный комплекс;
- ТК – технический комитет;
- УЦ – Удостоверяющий центр;
- ЭП – электронная подпись;
- ASN.1 - Abstract Syntax Notation One;
- CMC - Certificate Management over CMS;
- CMS – Cryptographic Message Syntax;
- CRL – Certificate Revocation List;
- ITU-T – International Telecommunication Union - Telecommunication sector;
- OOXML – Open Office XML;
- PDF – Portable Document Format;
- PAdES – PDF Advanced Electronic Signature;
- PIN – Personal Identification Number;
- REST - Representational State Transfer;
- RFC – Request for Comments;
- SOAP – Simple Object Access Protocol;
- XML – eXtensible Markup Language;
- OTP - One-Time Password;
- SMS - Short Message Service;
- STS - Security Token Service;
- TOTP - Time-Based One-Time Password Algorithm;
- HOTP - HMAC-Based One-Time Password Algorithm.

### 1.2. Термины и определения

В настоящем руководстве используются следующие термины:

- веб-сервис – реализация интерфейса взаимодействия между различными приложениями по протоколам SOAP и REST;
- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;
- сертификат ключа проверки электронной подписи – документ в электронном виде или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;
- 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.

## 2. ХАРАКТЕРИСТИКА ПРОГРАММЫ

Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам SOAP и REST.

В Cloud DSS поддерживаются следующие криптографические алгоритмы:

- алгоритм создания ключей электронной подписи ГОСТ Р 34.10-2012 [17];
- алгоритм электронной подписи ГОСТ Р 34.10-2012 [17];
- алгоритм шифрования ГОСТ 28147-89 [30].

Cloud DSS позволяет формировать запросы на создание сертификатов ключей проверки ЭП в формате PKCS #10 [7] и СМС [8].

Cloud DSS реализует следующие протоколы электронной подписи:

- CMS;
- CAdES;
- PAdES;
- XMLDSig;
- OOXML.

Cloud DSS реализует следующие протоколы шифрования данных:

- CMS.

Протокол CMS реализован в соответствии с RFC 5652 [2] и рекомендациями ТК 26 [14].

Протокол CAdES реализован в соответствии с RFC 5126 [5].

Протокол PAdES реализован в соответствии с [31].

Протокол XMLDSig реализован в соответствии с [4] и рекомендациями ТК 26 [15].

Протокол подписи документов OOXML реализован в соответствии с [32].

В Cloud DSS реализована возможность добавления меток доверенного времени в подпись в соответствии с CAdES [5], PAdES [31] и RFC 3161 [16].

Cloud DSS использует сертификаты ключей проверки ЭП в формате ITU-T X.509 [9] и рекомендаций ТК 26 [12].

### 3. ОБРАЩЕНИЕ К ПРОГРАММЕ

Взаимодействие с Cloud DSS осуществляется с помощью программных интерфейсов по протоколам SOAP и REST.

Для каждого веб-сервиса имена конечных точек интерфейса REST совпадают с именами методов интерфейса SOAP. Структуры, описывающие входные и выходные параметры для интерфейсов SOAP и REST также совпадают (см. п. 4).

Для обращения ко всем методам интерфейса REST используется HTTP метод POST.

Перед вызовом методов веб-сервиса необходимо получить на сервере идентификации маркер доступа (см. п. 6), который необходимо задавать при вызове методов веб-сервиса (см. п. 3.1.1). После истечения срока действия маркера, необходимо получить на сервере идентификации новый маркер доступа.

Операции (вызов методов) веб-сервисов могут выполняться в синхронном и асинхронном режиме (см. п. 3.2).

#### 3.1. Базовые структуры и типы данных

В данном разделе описаны общие для интерфейсов REST и SOAP структуры и базовые типы, используемые в методах веб-сервисов Cloud DSS.

##### 3.1.1. Структура RequestBaseType

Структура RequestBaseType является базовым типом для всех структур, используемых в качестве входных параметров методов веб-сервисов Cloud DSS.

Таблица 1 Описание полей структуры RequestBaseType

Поле	Тип	Описание
RequestID	String	Идентификатор запроса, уникальный для каждого вызова методов веб-сервиса.
Profile	String	Имя профиля конфигурации Cloud DSS. Если данное поле не задано, используется профиль по умолчанию [20].
OptionalInputs	OptionalInputsType	Дополнительные параметры запроса (см. Таблица 2).

Таблица 2 Описание полей структуры OptionalInputsType

Поле	Тип	Описание
AccessToken	String	Маркер доступа для выполнения операции, полученный на сервере идентификации (см. п. 6).
TransactionID	Integer	Идентификатор транзакции при выполнении асинхронной операции (см. п. 3.2).

##### 3.1.2. Структура ResponseBaseType

Структура ResponseBaseType является базовым типом для всех структур, используемых в качестве возвращаемых значений методов веб-сервиса Cloud DSS.

Таблица 3 Описание полей структуры ResponseBaseType

Поле	Тип	Описание
RequestID	String	Идентификатор запроса, заданный в структуре RequestBaseType.
Profile	String	Имя профиля конфигурации сервера Cloud DSS,



		используемого при обработке запроса.
Result	Result	Результат выполнения операции (см. Таблица 4).
OptionalOutputs	OptionalOutputsType	Дополнительные параметры ответа (см. Таблица 5).

Таблица 4 Описание полей структуры Result

Поле	Тип	Описание
ResultMajor	String	Основной параметр результата выполнения операции. Принимает следующие значения: Success – операция выполнена успешно; RequesterError – операция не выполнена из-за ошибки в запросе; ResponderError – операция не выполнена из-за ошибки на сервере.
ResultMinor	String	Вспомогательный параметр результата выполнения операции. Принимает следующие значения: OperationCompleted - операция завершена (ResultMajor равен Success); ConfirmationRequired – операция не завершена (ResultMajor равен Success), для завершения требуется подтверждение пользователя (см. п. 3.2); уточняющая информация об ошибке (ResultMajor равен RequesterError или ResponderError).

Таблица 5 Описание полей структуры OptionalOutputsType

Поле	Тип	Описание
TransactionID	Integer	Идентификатор транзакции. Возвращается в случае необходимости подтверждения операции пользователем (см. п. 3.2).

### 3.1.3. Структура KeySelectorType

Структура KeySelectorType используется для задания идентификатора ключа ЭП.

Таблица 6 Описание полей структуры KeySelectorType

Поле	Тип	Описание
KeyName	String	Уникальный идентификатор ключа ЭП для данного пользователя.

## 3.2. Синхронное и асинхронное выполнение операций

Под синхронным режимом выполнения операции подразумевается режим, при котором операция завершается при первом вызове метода веб-сервиса.

При успешном завершении операции поле ResultMajor возвращаемого значения будет равно Success, а ResultMinor – OperationCompleted (см. п. 3.1.2).

Если для выполнения операции (например, создания ЭП) требуется подтверждение пользователя (определяется настройками Cloud DSS), операция выполняется в асинхронном режиме: при первом успешном вызове метода возвращается уникальный идентификатор транзакции, который необходимо использовать при взаимодействии пользователя с сервером

идентификации для подтверждения операции (см. п.п. 6.1.3, 6.2.2). При этом поле ResultMajor возвращаемого значения будет равно Success, а ResultMinor – ConfirmationRequired.

После подтверждения операции пользователем, необходимо повторно вызвать тот же метод для завершения операции и получения результата, задав в соответствующем поле идентификатор транзакции (см. п. 3.1.1). Остальные параметры (за исключением маркера доступа) задавать не требуется: для завершения операции будут использованы параметры, заданные при первом вызове метода и сохраненные в базе данных Cloud DSS.

### 3.3. Интерфейс пользователя

Описание интерфейса SOAP веб-сервиса пользователя доступно по адресу:

`http://hostname[:port]/dss-customer-api/DSSCustomerWebService?wsdl`

hostname – адрес (IP или доменное имя) сервера приложений;

port – порт сервера приложений;

dss-customer-api – контекст веб-сервиса на сервере приложений.

Описание интерфейса REST веб-сервиса пользователя доступно по адресу:

`http://hostname[:port]/dss-customer-api/rest/application.wadl`

#### 3.3.1. Метод getCAInfo

Данный метод предназначен для получения информации об Удостоверяющих центрах, с которыми может взаимодействовать пользователь.

Параметры:

- getCAInfoRequest – структура GetCAInfoRequest (см. Таблица 7).

Таблица 7 Описание полей структуры GetCAInfoRequest

Поле	Тип	Описание
CA_ID	Integer	Идентификатор УЦ, по которому запрашивается информация. Если не задан, запрашивается информация по всем УЦ.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Возвращаемое значение: структура GetCAInfoResponse (см. Таблица 8).

Таблица 8 Описание полей структуры GetCAInfoResponse

Поле	Тип	Описание
CAs	CAInfoListType	Список параметров удостоверяющих центров (см. Таблица 9).

Таблица 9 Описание полей структуры CAInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество УЦ.
CA	List<CAInfoType>	Список объектов CAInfoType (см. Таблица 10).

Таблица 10 Описание полей структуры CAInfoType

Поле	Тип	Описание
CA_ID	Integer	Идентификатор УЦ.
DisplayName	String	Отображаемое название УЦ.
Parameters	CAParametersType	Дополнительные параметры УЦ (см. Таблица 11).
Locked	Boolean	True, если данный УЦ заблокирован.
CreationDate	DateTime	Дата создания записи.

Таблица 11 Описание полей структуры CAParametersType

Поле	Тип	Описание
NotaryPro	NotaryProParametersType	Параметры УЦ Notary-PRO (см. Таблица 12).

Таблица 12 Описание полей структуры NotaryProParametersType

Поле	Тип	Описание
ServiceUrl	String	Адрес веб-сервиса УЦ Notary-PRO.

### 3.3.2. Метод getCertificationRequestTemplateInfo

Данный метод предназначен для получения информации о шаблонах запросов на создание сертификата ключа проверки ЭП. Cloud DSS использует эти шаблоны для формирования запросов на создание сертификата ключа проверки ЭП (см. п. 3.3.4). Шаблоны «привязаны» к определенным УЦ. Удостоверяющему центру может принадлежать один или несколько шаблонов запросов на создание сертификата. Каждый шаблон предназначен для создания сертификата определенного типа, например, квалифицированного сертификата индивидуального предпринимателя.

Параметры:

- getCertificationRequestTemplateInfoRequest – структура GetCertificationRequestTemplateInfoRequest (см. Таблица 13).

Таблица 13 Описание полей структуры GetCertificationRequestTemplateInfoRequest

Поле	Тип	Описание
TemplateID	Integer	Идентификатор запрашиваемого шаблона. Если не задан, запрашивается список шаблонов.
ObjectFilter	ObjectFilterType	Фильтр объектов (см. Таблица 114). Допустимые поля фильтра для данной структуры см. Таблица 14.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Таблица 14 Допустимые поля фильтра объектов структуры GetCertificationRequestTemplateInfoRequest

Поле	Тип	Описание
CAId	Integer	Идентификатор Удостоверяющего центра.

Возвращаемое значение: структура GetCertificationRequestTemplateInfoResponse (см. Таблица 15).

Таблица 15 Описание полей структуры GetCertificationRequestTemplateInfoResponse

Поле	Тип	Описание
CertificationRequestTemplates	CertificationRequestTemplateInfoListType	Список шаблонов (см. Таблица 16).

Таблица 16 Описание полей структуры CertificationRequestTemplateInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество шаблонов.
CertificationRequestTemplate	List< CertificationRequestTemplateInfoType >	Список объектов CertificationRequestTemplateInfoType (см. Таблица 17).

Таблица 17 Описание полей структуры CertificationRequestTemplateInfoType

Поле	Тип	Описание
TemplateID	Integer	Идентификатор шаблона.
DisplayName	String	Отображаемое название шаблона.
CAId	Integer	Идентификатор УЦ.
KeyAlgorithm	KeyAlgorithmType	Параметры ключей ЭП (см. Таблица 20).
X509NamePolicy	List<X509NamePolicyAttributeType>	Список атрибутов имени владельца в запросе на сертификат (см. Таблица 18).
X509CertificatePolicies	List<String>	Список стандартных идентификаторов расширения сертификата Certificate Policies, заданных в соответствии с правилами RFC 3061, например:  "urn:oid:1.2.643.100.113.1" - класс средства ЭП КС1;  "urn:oid:1.2.643.100.113.2" - класс средства ЭП КС2.
X509ExtendedKeyUsage	List<String>	Список стандартных идентификаторов расширения сертификата Extended Key Usage, заданных в соответствии с правилами RFC 3061, например:  "urn:oid:1.3.6.1.5.5.7.3.4" - защита электронной почты.
IncludeSubjectSignTool	Boolean	Управляет заданием расширения квалифицированного сертификата subjectSignTool (наименование используемого

		владельцем квалифицированного сертификата средства ЭП).
Locked	Boolean	True, если данный шаблон заблокирован.
CreationDate	DateTime	Дата создания шаблона.

Таблица 18 Описание полей структуры X509NamePolicyAttributeType

Поле	Тип	Описание
Oid	String	Стандартный идентификатор атрибута имени в соответствии с правилами RFC 3061, например: "urn:oid:2.5.4.6" – countryName; "urn:oid:2.5.4.7" – localityName; "urn:oid:2.5.4.9" – streetAddress; "urn:oid:2.5.4.10" – organizationName.
required	Boolean	True, если данный атрибут является обязательным, и false, если не является. По умолчанию – true.

### 3.3.3. Метод generateKeyPair

Данный метод предназначен для создания ключа ЭП и ключа проверки ЭП, дополнительно можно сформировать запрос на создание сертификата ключа проверки ЭП в формате PKCS #10 [7] или СМС [8].

Параметры:

- generateKeyPairRequest – структура GenerateKeyPairRequest (см. Таблица 19).

Таблица 19 Описание полей структуры GenerateKeyPairRequest

Поле	Тип	Описание
KeyAlgorithm	KeyAlgorithmType	Параметры ключей ЭП (см. Таблица 20). Если данное поле не задано, используются параметры по умолчанию.
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3). Если данное поле не задано, идентификатор ключа формируется на сервере Cloud DSS.
CertificationRequestInfo	CertificationRequestInfoType	Параметры запроса на сертификат ключа проверки ЭП (см. Таблица 24). Если данное поле задано, формируется запрос на создание сертификата для нового ключа проверки ЭП в формате PKCS #10 или СМС (см. п. 3.3.4)..

Label	String	Метка ключа ЭП. Необязательный параметр.
-------	--------	--

Таблица 20 Описание полей структуры KeyAlgorithmType

Поле	Тип	Описание
Algorithm	String	Идентификатор алгоритма ключей ЭП. Задается в соответствии с правилами RFC 3061, может принимать следующие значения:  "urn:oid:1.2.643.7.1.1.1.1" - алгоритм ГОСТ Р 34.10-2012 [17] с длиной хэш-кода 256 бит;  "urn:oid:1.2.643.7.1.1.1.2" - алгоритм ГОСТ Р 34.10-2012 [17] с длиной хэш-кода 512 бит.
GOSTKeyParameters	GOSTKeyParametersType	Параметры ключей ЭП алгоритма ГОСТ Р 34.10-2012 (см. Таблица 21). Если данное поле не задано, используются параметры по умолчанию.

Таблица 21 Описание полей структуры GOSTKeyParameters

Поле	Тип	Описание
ParamSet	String	Идентификатор набора параметров ключей ЭП алгоритма ГОСТ. Задается в соответствии с правилами RFC 3061.  Для алгоритма "urn:oid:1.2.643.7.1.1.1.1" может принимать следующие значения:  "urn:oid:1.2.643.2.2.35.1" - параметры id-GostR3410-2001-CryptoPro-A-ParamSet [11] (значение по умолчанию);  "urn:oid:1.2.643.2.2.35.2" - параметры id-GostR3410-2001-CryptoPro-B-ParamSet [11];  "urn:oid:1.2.643.2.2.35.3" - параметры id-GostR3410-2001-CryptoPro-C-ParamSet [11];  "urn:oid:1.2.643.2.2.36.0" - параметры id-GostR3410-2001-CryptoPro-XchA-ParamSet [11];  "urn:oid:1.2.643.2.2.36.1" - параметры id-GostR3410-2001-CryptoPro-XchB-ParamSet [11];  "urn:oid:1.2.643.7.1.2.1.1.1" - параметры id-tc26-gost-3410-12-256-paramSetA [23];  "urn:oid:1.2.643.7.1.2.1.1.2" - параметры id-tc26-gost-3410-12-256-paramSetB [23];  "urn:oid:1.2.643.7.1.2.1.1.3" - параметры id-tc26-gost-3410-12-256-paramSetC [23];  "urn:oid:1.2.643.7.1.2.1.1.4" - параметры

		id-tc26-gost-3410-12-256-paramSetD [23].  Для алгоритма "urn:oid:1.2.643.7.1.1.1.2" может принимать следующие значения:  "urn:oid:1.2.643.7.1.2.1.2.1" - параметры id-tc26-gost-3410-12-512-paramSetA [13] (значение по умолчанию);  "urn:oid:1.2.643.7.1.2.1.2.2" - параметры id-tc26-gost-3410-12-512-paramSetB [13];  "urn:oid:1.2.643.7.1.2.1.2.3" - параметры id-tc26-gost-3410-12-512-paramSetC [23].
--	--	---

Возвращаемое значение: структура GenerateKeyPairResponse (см. Таблица 22).

Таблица 22 Описание полей структуры GenerateKeyPairResponse

Поле	Тип	Описание
KeySelector	KeySelectorType	Идентификатор созданного ключа ЭП в случае успешного завершения операции (см. п. 3.1.3).

### 3.3.4. Метод generateCertificationRequest

Данный метод предназначен для создания запроса на создание сертификата ключа проверки ЭП в формате PKCS #10 [7] или СМС [8]. В случае успешного завершения операции созданный запрос на создание сертификата помещается в базу данных Cloud DSS.

Запрос на создание сертификата ключа проверки ЭП в формате PKCS #10 может быть отправлен в Удостоверяющий центр, зарегистрированный в Cloud DSS. Для этого необходимо в параметрах метода задать идентификатор ключа ЭП (см. п.п. 3.1.3, 3.3.3 и 3.3.5), идентификатор УЦ (см. п. 3.3.1) и идентификатор шаблона этого УЦ (см. п. 3.3.2). В случае успешного завершения операции можно проверить статус обработки запроса на создание сертификата ключа проверки ЭП и загрузить изготовленный Удостоверяющим центром сертификат ключа проверки ЭП (см. п. 3.3.5).

Если запрос на создание сертификата ключа проверки ЭП в формате PKCS #10 формируется для Удостоверяющего центра, не зарегистрированного в Cloud DSS, необходимо в параметрах метода задать идентификатор ключа ЭП, имя владельца в запросе на сертификат ключа проверки ЭП и расширения сертификата (опционально). Идентификатор Удостоверяющего центра задавать не нужно. В случае успешного завершения операции созданный запрос на создание сертификата может быть экспортирован из базы данных Cloud DSS в файл для дальнейшей доставки во внешний Удостоверяющий центр.

Запрос в формате СМС используется для обновления действующего сертификата ключа проверки ЭП. Для формирования запроса в формате СМС необходимо задать идентификатор нового ключа ЭП и идентификатор ключа проверки ЭП обновляемого сертификата. Если обновляемый сертификат ключа проверки ЭП выпущен Удостоверяющим центром, зарегистрированным в Cloud DSS, сформированный запрос на создание сертификата ключа проверки ЭП автоматически отправляется в этот же УЦ. В случае успешного завершения операции можно проверить статус обработки запроса на создание сертификата ключа проверки ЭП и загрузить изготовленный Удостоверяющим центром сертификат ключа проверки ЭП (см. п. 3.3.5).

Параметры:

- generateCertificationRequestRequest – структура GenerateCertificationRequestRequest (см. Таблица 23).

Таблица 23 Описание полей структуры GenerateCertificationRequestRequest

Поле	Тип	Описание
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3).
CertificationRequestInfo	CertificationRequestInfoType	Параметры запроса на создание сертификата ключа проверки ЭП (см. Таблица 24).

Таблица 24 Описание полей структуры CertificationRequestInfoType

Поле	Тип	Описание
X509SubjectName	X509NameType	Имя владельца в запросе на сертификат ключа проверки ЭП. Может быть задано в виде строки, соответствующей правилам RFC 4514 [18], или в виде списка атрибутов имени (см. Таблица 25).
X509Extensions	X509ExtensionsType	Расширения сертификата (см. Таблица 28).
SignatureKey	KeySelectorType	Идентификатор ключа ЭП для подписи СМС-запроса. Если данное поле задано, запрос на создание сертификата ключа проверки ЭП создается в формате СМС [8], если не задано – в формате PKCS #10 [7].
AddSignerCertificate	Boolean	Используется при создании запроса на создание сертификата в формате СМС и управляет включением сертификата ключа проверки ЭП в ЭП СМС-запроса (по умолчанию сертификат включается).
CAId	Integer	Идентификатор Удостоверяющего центра (см. п. 3.3.1), в который Cloud DSS должен отправить запрос на создание сертификата ключа проверки ЭП.
TemplateId	Integer	Идентификатор шаблона запроса на создание сертификата ключа проверки ЭП (см. п. 3.3.2).

Таблица 25 Описание полей структуры X509NameType

Поле	Тип	Описание
X509Name	String	Имя владельца, заданное в виде строки, соответствующей правилам RFC 4514 [18].
X509NameAttributes	X509NameAttributes	Имя владельца в виде списка атрибутов имени (см. Таблица 26).

Таблица 26 Описание полей структуры X509NameAttributes

Поле	Тип	Описание
509NameAttribute	List<509NameAttribute>	Список объектов 509NameAttribute (см. Таблица 27).



Таблица 27 Описание полей структуры 509NameAttribute

Поле	Тип	Описание
oid	String	Стандартный идентификатор атрибута имени в соответствии с правилами RFC 3061, например: "urn:oid:2.5.4.6" – countryName; "urn:oid:2.5.4.7" – localityName; "urn:oid:2.5.4.9" – streetAddress; "urn:oid:2.5.4.10" – organizationName.
value	String	Значение атрибута.

Таблица 28 Описание полей структуры X509ExtensionsType

Поле	Тип	Описание
CertificatePolicy	List<String>	Список стандартных идентификаторов расширения сертификата Certificate Policies, заданных в соответствии с правилами RFC 3061, например: "urn:oid:1.2.643.100.113.1" - класс средства ЭП КС1; "urn:oid:1.2.643.100.113.2" - класс средства ЭП КС2.
ExtendedKeyUsage	List<String>	Список стандартных идентификаторов расширения сертификата Extended Key Usage, заданных в соответствии с правилами RFC 3061, например: "urn:oid:1.3.6.1.5.5.7.3.4" - защита электронной почты.
IncludeSubjectSignTool	Boolean	Управляет заданием расширения квалифицированного сертификата subjectSignTool (наименование используемого владельцем квалифицированного сертификата средства ЭП).

Возвращаемое значение: структура GenerateCertificationRequestResponse (см. п. 3.1.2).

### 3.3.5. Метод getKeyEntryInfo

Данный метод предназначен для получения информации о ключах ЭП, запросах на создание сертификатов ключей проверки ЭП, сертификатах ключей проверки ЭП и запросах на аннулирование сертификатов ключей проверки ЭП.

Перед выдачей этой информации выполняется обращение к веб-сервису Удостоверяющего центра для получения актуальных статусов объектов и загрузки созданных сертификатов ключей проверки ЭП.

Параметры:

- getKeyEntryInfoRequest – структура GetKeyEntryInfoRequest (см. Таблица 29).

Таблица 29 Описание полей структуры GetKeyEntryInfoRequest

Поле	Тип	Описание
------	-----	----------

KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3). Если поле не задано, выдается информация по всем ключам ЭП пользователя.
ResultFormat	String	Формат кодирования получаемых параметров (запросов на создание сертификата, сертификатов и запросов на аннулирование сертификатов):  "ASN.1" – формат ASN.1 (используется по умолчанию);  "PEM" – формат PEM.

Возвращаемое значение: структура GetKeyEntryInfoResponse (см. Таблица 30).

Таблица 30 Описание полей структуры GetKeyEntryInfoResponse

Поле	Тип	Описание
KeyEntries	KeyEntryInfoListType	Описывает список структур с параметрами ключей ЭП (см. Таблица 31).

Таблица 31 Описание полей структуры KeyEntryInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество ключей ЭП.
KeyEntry	List<KeyEntryInfoType>	Список объектов KeyEntryInfoType (см. Таблица 32).

Таблица 32 Описание полей структуры KeyEntryInfoType

Поле	Тип	Описание
KeyName	String	Идентификатор ключа ЭП. Соответствует полю KeyName структуры KeySelectorType (см. п. 3.1.3).
Label	String	Метка (псевдоним) ключа ЭП.
PrivateKeyStartDate	DateTime	Дата начала действия ключа ЭП.
PrivateKeyEndDate	DateTime	Дата окончания действия ключа ЭП.
CertificationRequest	CertificationRequestType	Информация о запросе на сертификат ключа проверки ЭП (см. Таблица 33).
X509Certificate	X509CertificateType	Информация о сертификате ключа проверки ЭП (см. Таблица 34).
RevocationRequest	RevocationRequestType	Информация о запросе на аннулирование сертификата ключа проверки ЭП (см. Таблица 37).

Таблица 33 Описание полей структуры CertificationRequestType

Поле	Тип	Описание
EncodedRequest	byte[]	Запрос на сертификат ключа проверки ЭП, закодированный в соответствии с параметром ResultFormat (см. Таблица

		29).
Status	String	Статус запроса на создание сертификата. Может принимать следующие значения:  INITIAL – запрос помещен в базу данных Cloud DSS;  PENDING – запрос ожидает отправки в УЦ;  ACCEPTED – запрос принят на обработку в УЦ;  REJECTED – запрос отклонен УЦ;  CERTIFIED – запрос сертифицирован УЦ.
Subject	String	Имя владельца в виде строки, соответствующей правилам RFC 4514 [18].
CAId	Integer	Идентификатор Удостоверяющего центра.
UserID	Integer	Идентификатор пользователя.
KeyName	String	Идентификатор ключа ЭП (см. п. 3.1.3).
ErrorMessage	String	Строка ошибки, если статус запроса на создание сертификата – REJECTED.

Таблица 34 Описание полей структуры X509CertificateType

Поле	Тип	Описание
EncodedCertificate	byte[]	Сертификат ключа проверки ЭП, закодированный в соответствии с параметром ResultFormat (см. Таблица 29).
CertificateStatus	X509CertificateStatusType	Информация о статусе сертификата ключа проверки ЭП (см. Таблица 35).
Subject	String	Имя владельца в виде строки, соответствующей правилам RFC 4514 [18].
Issuer	String	Имя издателя (УЦ) в виде строки, соответствующей правилам RFC 4514.
NotBefore	DateTime	Дата начала действия сертификата.
NotAfter	DateTime	Дата окончания действия сертификата.
CAId	Integer	Идентификатор Удостоверяющего центра.
UserID	Integer	Идентификатор пользователя.
KeyName	String	Идентификатор ключа ЭП (см. п. 3.1.3).

Таблица 35 Описание полей структуры X509CertificateStatusType

Поле	Тип	Описание
Status	String	Статус сертификата. Может принимать следующие значения:

		ACTIVE – сертификат действителен; REVOKED – сертификат аннулирован; HOLD – действие сертификата приостановлено; NOT_VALID – сертификат не действителен.
RevocationInfo	RevocationInfoType	Информация об аннулировании сертификата (см. Таблица 36).

Таблица 36 Описание полей структуры RevocationInfoType

Поле	Тип	Описание
Reason	Integer	Код причины аннулирования сертификата (см. RFC 5280).
InvalidityDate	DateTime	Дата аннулирования сертификата.
Comment	String	Комментарий к запросу на аннулирование.

Таблица 37 Описание полей структуры RevocationRequestType

Поле	Тип	Описание
EncodedRequest	byte[]	Запрос на аннулирование сертификата ключа проверки ЭП, закодированный в соответствии с параметром ResultFormat (см. Таблица 29).
Status	String	Статус запроса на аннулирование сертификата. Может принимать следующие значения:  INITIAL – запрос помещен в базу данных Cloud DSS;  PENDING – запрос ожидает отправки в УЦ;  ACCEPTED – запрос принят на обработку в УЦ;  REJECTED – запрос отклонен УЦ;  PROCESSED – запрос обработан УЦ.
CAId	Integer	Идентификатор Удостоверяющего центра.
UserID	Integer	Идентификатор пользователя.
KeyName	String	Идентификатор ключа ЭП (см. п. 3.1.3).
ErrorMessage	String	Строка ошибки, если статус запроса на аннулирование – REJECTED.

### 3.3.6. Метод updateKeyEntryInfo

Данный метод предназначен для выполнения одной из следующих операций: помещения сертификата ключа проверки ЭП в хранилище Cloud DSS, аннулирования сертификата ключа проверки ЭП, задания или смены метки (псевдонима) ключа ЭП.

Параметры:

- updateKeyEntryInfoRequest – структура UpdateKeyEntryInfoRequest (см. Таблица 38).

Таблица 38 Описание полей структуры UpdateKeyEntryInfoRequest

Поле	Тип	Описание
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3). Данное поле может отсутствовать, если метод используется для помещения сертификата ключа проверки ЭП.
UpdatedKeyEntryInfo	UpdatedKeyEntryInfoType	В данном поле задается только один из допустимых параметров ключа ЭП (см. Таблица 39).

Таблица 39 Описание полей структуры UpdatedKeyEntryInfoType

Поле	Тип	Описание
X509Certificate	byte[]	Сертификат ключа проверки ЭП.
X509CertificateStatus	X509CertificateStatusType	Информация о статусе сертификата ключа проверки ЭП (см. Таблица 35).
Label	String	Метка (псевдоним) ключа ЭП.

Возвращаемое значение: структура UpdateKeyEntryInfoResponse (см. п. 3.1.2).

### 3.3.7. Метод deleteKeyEntry

Данный метод предназначен для удаления ключа ЭП. При этом удаляются запрос на создание сертификата, сертификат и запрос на аннулирование сертификата для этого ключа, если эти объекты существуют.

Параметры:

- deleteKeyEntryRequest – структура DeleteKeyEntryRequest (см. Таблица 40).

Таблица 40 Описание полей структуры DeleteKeyEntryRequest

Поле	Тип	Описание
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3).

Возвращаемое значение: структура DeleteKeyEntryResponse (см. п. 3.1.2).

### 3.3.8. Метод getTokenInfo

Данный метод предназначен для получения информации о виртуальном токене.

Параметры:

- getTokenInfoRequest – структура GetTokenInfoRequest (см. п. 3.1.1).

Возвращаемое значение: структура GetTokenInfoResponse (см. Таблица 41).

Таблица 41 Описание полей структуры GetTokenInfoResponse

Поле	Тип	Описание
TokenInfo	TokenInfoType	Параметры виртуального токена (см. Таблица 42).

Таблица 42 Описание полей структуры TokenInfoType

Поле	Тип	Описание
------	-----	----------

Label	String	Метка.
MaxPinLen	Integer	Максимальная длина PIN-кода.
MinPinLen	Integer	Минимальная длина PIN-кода.
TotalPublicMemory	Integer	Общий размер незащищенной памяти.
FreePublicMemory	Integer	Размер доступной незащищенной памяти.
TotalPrivateMemory	Integer	Общий размер защищенной памяти.
FreePrivateMemory	Integer	Размер доступной защищенной памяти.
PinLocked	Boolean	True, если PIN-код заблокирован.
PinToBeChanged	Boolean	True, если PIN-код должен быть изменен.
PinCountLow	Boolean	True, если со времени последней успешной аутентификации пользователь по крайней мере один раз ввел неверный PIN-код.
PinFinalTry	Boolean	True, если последующий ввод неверного PIN-кода приведет к его блокированию.
SerialNumber	String	Серийный номер
MaxPrivateMemory	Integer	Максимальный допустимый размер защищенной памяти при создании виртуального токена.
MaxPublicMemory	Integer	Максимальный допустимый размер незащищенной памяти при создании виртуального токена.

### 3.3.9. Метод updateTokenInfo

Данный метод предназначен для выполнения одной из следующих операций: изменения метки, смены PIN-кода виртуального токена.

Для смены PIN-кода виртуального токена необходимо в поле TokenInfo входных параметров задать значение PinToBeChanged равным true. После вызова данного метода необходимо выполнить на сервере идентификации процедуру завершения сессии (см. п. 6.1.7), а затем процедуру получения маркера доступа (см. п. 6.1), в процессе которой пользователь будет перенаправлен на страницу сервера идентификации для ввода нового PIN-кода виртуального токена.

Параметры:

- updateTokenInfoRequest – структура UpdateTokenInfoRequest (см. Таблица 43).

Таблица 43 Описание полей структуры UpdateTokenInfoRequest

Поле	Тип	Описание
TokenInfo	TokenInfoType	Новое значение Label или PinToBeChanged равный true (см. Таблица 42).

Возвращаемое значение: структура UpdateTokenInfoResponse (см. п. 3.1.2).

### 3.3.10. Метод sign

Данный метод предназначен для создания ЭП и добавления метки доверенного времени в ЭП.

Параметры:

- signRequest – структура SignRequest (см. Таблица 44).

Таблица 44 Описание полей структуры SignRequest

Поле	Тип	Описание
InputDocument	InputDocumentType	Подписываемые данные (см. Таблица 45).
SignatureType	String	Тип ЭП. Может принимать следующие значения: CMS - ЭП в формате CMS (по умолчанию), см. [2]; XMLDSIG - ЭП в формате XMLDSig (см. [4]); PADES – ЭП в формате PAdES [31]; OOXML – ЭП в формате OOXML [32].
SignParameters	SignParametersType	Параметры подписи (см. Таблица 50).
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3).
AddTimestamp	AddTimestampType	Если поле задано, необходимо добавить в ЭП метку доверенного времени (см. Таблица 56).

Таблица 45 Описание полей структуры InputDocumentType

Поле	Тип	Описание
Document	DocumentType	Подписать заданный документ (см. Таблица 46).
DocumentHash	DocumentHashType	Подписать заданное хэш-значение (см. Таблица 48).
Name	String	Название или краткое содержание документа. Эти данные будут отображаться в веб-интерфейсе сервера идентификации и передаваться в сообщении пользователю (SMS, Email и т.д.) при подтверждении операции создания ЭП (см. п. 6.1.3). Максимальный размер данного параметра не может превышать 256 символов.

Таблица 46 Описание полей структуры DocumentType

Поле	Тип	Описание
Base64Data	Base64Data	Параметры документа (см. Таблица 47).

Таблица 47 Описание полей структуры Base64Data

Поле	Тип	Описание
MimeType	String	Тип документа.

Value	byte[]	Содержимое документа.
-------	--------	-----------------------

Таблица 48 Описание полей структуры DocumentHashType

Поле	Тип	Описание
DigestMethod	DigestMethodType	Параметры хэш-алгоритма (см. Таблица 49).
DigestValue	byte[]	Хэш-значение.

Таблица 49 Описание полей структуры DigestMethodType

Поле	Тип	Описание
Algorithm	String	Идентификатор хэш-алгоритма.

Таблица 50 Описание полей структуры SignParametersType

Поле	Тип	Описание
CMSSignParameters	CMSSignParametersType	Параметры ЭП формата CMS (см. Таблица 51).
XMLSignParameters	XMLSignParametersType	Параметры ЭП формата XMLDSig (см. Таблица 52).
PDFSignParameters	PDFSignParametersType	Параметры ЭП формата PAdES (см. Таблица 57).
OOXMLSignParameters	OOXMLSignParametersType	Параметры ЭП формата OOXML (см. Таблица 67).

Таблица 51 Описание полей структуры CMSSignParametersType

Поле	Тип	Описание
Detached	Boolean	True, если формируется отсоединенная ЭП (по умолчанию). False – присоединенная.

Таблица 52 Описание полей структуры XMLSignParametersType

Поле	Тип	Описание
SignatureType	String	Тип ЭП в формате XMLDSig. Может принимать следующие значения: Enveloped – вложенная подпись; Detached – отсоединенная подпись.
SignaturePlacement	SignaturePlacement	Место расположения элемента ЭП внутри заданного XML-документа (см. Таблица 53).
SignedReferences	SignedReferences	Подписываемые данные и алгоритмы их обработки (см. Таблица 54).

Таблица 53 Описание полей структуры SignaturePlacement

Поле	Тип	Описание
XPathAfter	String	XPath-выражение (см. [6]), которое определяет элемент, после которого будет вставлена ЭП.
XPathFirstChildOf	String	XPath-выражение (см. [6]), которое



		определяет элемент, в который будет вставлена ЭП как первый дочерний элемент. ЭП помещается сразу после начального тега указанного элемента.
--	--	--

Таблица 54 Описание полей структуры SignedReferences

Поле	Тип	Описание
SignedReference	List<SignedReferenceType>	Список объектов SignedReferenceType (см. Таблица 55).

Таблица 55 Описание полей структуры SignedReferenceType

Поле	Тип	Описание
RefURI	String	Соответствует атрибуту URI элемента <ds:Reference> (см. [4]).
RefId	String	Соответствует атрибуту Id элемента <ds:Reference> (см. [4]).
Transforms	TransformsType	Соответствует элементу <ds:Transforms> (см. [4]).

Таблица 56 Описание полей структуры AddTimestampType

Поле	Тип	Описание
TimeStampTheGivenSignature	Boolean	True, если необходимо сформировать метку доверенного времени для уже существующей ЭП. По умолчанию метка доверенного времени формируется для вновь создаваемой ЭП.

Таблица 57 Описание полей структуры PDFSignParametersType

Поле	Тип	Описание
Name	String	Имя лица или органа, подписавшего документ.
Reason	String	Причина подписания документа.
Location	String	Физическое расположение, где был подписан документ.
ContactInfo	String	Контактная информация лица или органа, подписавшего документ.
DocMDP	DocMDPType	Используется для создания сертифицирующей (certification) ЭП (см. Таблица 58). По умолчанию создается одобряющая (approval) ЭП.
VisibleSignature	PDFVisibleSignatureType	Используется для создания видимой ЭП (см. Таблица 59). По умолчанию создаётся невидимая ЭП.

Таблица 58 Описание полей структуры DocMDPType

Поле	Тип	Описание
P	Integer	Ограничения по модификации

		<p>документа после создания сертифицирующей (certification) ЭП. Может принимать следующие значения:</p> <p>1 – изменения документа запрещены;</p> <p>2 – разрешены операции заполнения формы, подписи и добавления страниц;</p> <p>3 - разрешены операции комментирования, заполнения формы, подписи и добавления страниц.</p>
--	--	--

Таблица 59 Описание полей структуры PDFVisibleSignatureType

Поле	Тип	Описание
BottomTextSignature	BottomTextSignatureType	Параметры текстового представления подписи под документом (см. Таблица 60). Если параметры не заданы, используются параметры, задаваемые в конфигурации сервера.

Таблица 60 Описание полей структуры BottomTextSignatureType

Поле	Тип	Описание
Alignment	String	Параметр выравнивания. Может принимать следующие значения: «Center» - по центру; «Left» - по левому краю; «Right» - по правому краю.
Rectangle	RectangleType	Параметры прямоугольника (см. Таблица 61).
Border	BorderType	Параметры рамки (см. Таблица 62).
Background	BackgroundType	Параметры фона (см. Таблица 63).
Text	TextType	Параметры текста (см. Таблица 64).

Таблица 61 Описание полей структуры RectangleType

Поле	Тип	Описание
Space	Integer	Расстояние прямоугольника от текста документа в точках (1/72 дюйма).
Width	Integer	Ширина прямоугольника в точках.
Height	Integer	Высота прямоугольника в точках.

Таблица 62 Описание полей структуры BorderType

Поле	Тип	Описание
Color	RGBColorType	Цвет (см. Таблица 65).

Таблица 63 Описание полей структуры BackgroundType

Поле	Тип	Описание
Color	RGBColorType	Цвет (см. Таблица 65).

Таблица 64 Описание полей структуры TextType

Поле	Тип	Описание
Color	RGBColorType	Цвет (см. Таблица 65).
Font	FontType	Шрифт (см. Таблица 66).
Leading	String	Расстояние между строками текста в точках (float в строковом представлении, например, "1.5").

Таблица 65 Описание полей структуры RGBColorType

Поле	Тип	Описание
Red	Integer	Значение красного (0 - 255).
Green	Integer	Значение зеленого (0 - 255).
Blue	Integer	Значение синего (0 - 255).

Таблица 66 Описание полей структуры FontType

Поле	Тип	Описание
Name	String	Имя шрифта.
Size	String	Размер шрифта в точках (float в строковом представлении, например, "6.0").

Таблица 67 Описание полей структуры OOXMLSignParametersType

Поле	Тип	Описание
SignerRole	String	Роль лица, подписывающего документ, в организации.
CommitmentIndication	CommitmentIndicationType	Описывает обязательства, взятые на себя подписывающей стороной (см. Таблица 68).
SignatureProductionPlace	SignatureProductionPlaceType	Задаёт предполагаемое место, где находилось лицо во время подписания документа (см. Таблица 69).

Таблица 68 Описание полей структуры CommitmentIndicationType

Поле	Тип	Описание
Identifier	String	Идентификатор обязательства.
Description	String	Описание обязательства.
Qualifier	String	Квалификатор, может предоставлять дополнительную информацию об обязательстве.

Таблица 69 Описание полей структуры SignatureProductionPlaceType

Поле	Тип	Описание
City	String	Город.
StateOrProvince	String	Область.

PostalCode	String	Почтовый код.
CountryName	String	Страна.

Возвращаемое значение: структура SignResponse (см. Таблица 70).

Таблица 70 Описание полей структуры SignResponse

Поле	Тип	Описание
SignatureObject	SignatureObjectType	Объект подписи (см. Таблица 71).
DocumentWithSignature	DocumentWithSignatureType	XML-документ, содержащий ЭП. Данное поле используется только для ЭП в формате XMLDSig (см. Таблица 74).

Таблица 71 Описание полей структуры SignatureObjectType

Поле	Тип	Описание
Base64Signature	Base64Signature	Отсоединенная ЭП (CMS или XMLDSig) или ЭП с включенными данными в формате CMS (см. Таблица 72).
SignaturePtr	SignaturePtr	Ссылка на элемент ЭП в XML-документе (см. Таблица 73). Данное поле используется только для ЭП в формате XMLDSig.

Таблица 72 Описание полей структуры Base64Signature

Поле	Тип	Описание
Type	String	Тип ЭП (см. Таблица 44).
Value	byte[]	Значение ЭП.

Таблица 73 Описание полей структуры SignaturePtr

Поле	Тип	Описание
XPath	String	XPath-выражение (см. [6]), которое определяет расположение элемента ЭП в XML-документе.

Таблица 74 Описание полей структуры DocumentWithSignatureType

Поле	Тип	Описание
Document	DocumentType	XML-документ, содержащий ЭП (см. Таблица 46).

### 3.3.10.1 Создание ЭП в формате CMS

Подписываемые данные необходимо указать в поле InputDocument.

По умолчанию подписываемые данные не включаются в ЭП, т. е. формируется отсоединенная ЭП. Для включения данных в ЭП необходимо в структуре CMSSignParameters задать поле Detached, равным false.

---

При успешном выполнении операции значение ЭП возвращается в поле SignatureObject (поле Value структуры Base64Signature).

Создаваемая ЭП имеет форму CAdES-BES, т. е. удовлетворяет требованиям п. 4.3.1 [5].

### **3.3.10.2 Создание ЭП в формате CMS с добавлением метки доверенного времени**

Если Cloud DSS соответствующим образом сконфигурирован, он может сразу после создания ЭП добавить в нее метку доверенного времени.

Для этого необходимо задать поле AddTimestamp (поле TimeStampTheGivenSignature не задается).

Метка доверенного времени добавляется в ЭП как неподписанный атрибут с идентификатором 1.2.840.11359.1.9.16.2.14 согласно RFC 5126 [5].

Все остальные элементы кодируются как описано в п. 3.3.10.1.

### **3.3.10.3 Добавление метки доверенного времени в CMS подпись**

Если Cloud DSS соответствующим образом сконфигурирован, он может добавить метку доверенного времени в уже существующую ЭП.

Для этого необходимо задать поле AddTimestamp, значение поля TimeStampTheGivenSignature должно быть равно true.

ЭП должна быть указана в поле InputDocument (поле Base64Data структуры Document).

Метка доверенного времени добавляется в ЭП как неподписанный атрибут с идентификатором 1.2.840.11359.1.9.16.2.14 согласно RFC 5126 [5].

При успешном выполнении операции модифицированное значение ЭП возвращается в поле SignatureObject (поле Value структуры Base64Signature).

### **3.3.10.4 Создание ЭП в формате XMLDSig**

Для этого необходимо задать поле SignatureType равным XMLDSIG.

Исходный XML-документ (если есть) указывается в поле InputDocument (поле Base64Data структуры Document).

По умолчанию формируется вложенная ЭП. Для формирования отсоединенной ЭП, необходимо в поле SignatureType структуры XMLSignParameters задать значение Detached.

Подписываемые данные указываются в поле SignedReferences структуры XMLSignParameters, которое должно содержать не менее одного объекта SignedReference.

Объект SignedReference должен содержать атрибут RefURI, имеющий одно из следующих значений:

- "" (пустая строка) – ссылка на весь XML-документ, заданный в InputDocument;
- значение, начинающееся с символа '#' – ссылка на часть XML-документа, заданного в InputDocument (например, RefURI="#some-id");
- внешняя ссылка (например, <http://www.example.com/index.html>).

Объект SignedReference может содержать поле Transforms с произвольным числом объектов Transform, описывающих дополнительные преобразования данных перед подписанием.

Поля XPathFirstChildOf и XPathAfter структуры SignaturePlacement представляют собой XPath-выражения [6] и могут задавать место расположения ЭП в XML-документе.

При успешном выполнении операции документ с ЭП возвращается в поле DocumentWithSignature.

### 3.3.10.5 Создание ЭП документа в формате PDF

Для этого необходимо задать поле `SignatureType` равным `PADES`.

Подписываемый документ в формате PDF должен быть указан в поле `InputDocument` (поле `Base64Data` структуры `Document`).

Свойства электронной подписи должны быть заданы в поле `PDFSignParameters` структуры `SignParameters` (см. Таблица 57).

По умолчанию создаётся невидимая электронная подпись. Для создания видимой электронной подписи необходимо в структуре `PDFSignParameters` задать поле `VisibleSignature` (см. Таблица 59). При отсутствии в структуре `VisibleSignature` полей видимой электронной подписи используются параметры, задаваемые конфигурацией сервера. Содержание видимой ЭП соответствует требованиям ст. 12, ч.3 Федерального закона "Об электронной подписи" от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) [33]. При создании нескольких видимых ЭП в документе должно быть достаточно места для их размещения, при недостатке места возвращается ошибка.

По умолчанию создаётся одобряющая (`approval`) электронная подпись. Для создания сертифицирующей (`certification`) электронной подписи необходимо задать поле `DocMDP` структуры `PDFSignParameters` (см. Таблица 58).

Если сервер сконфигурирован соответствующим образом, то он может сразу после создания ЭП добавить в подпись метку доверенного времени.

Для этого необходимо задать поле `AddTimestamp` (поле `TimeStampTheGivenSignature` не задается).

Метка доверенного времени добавляется в подпись как неподписанный атрибут `signature-time-stamp` с идентификатором 1.2.840.11359.1.9.16.2.14.

Документ в формате PDF с электронной подписью при успешном результате выполнения операции возвращается в поле `SignatureObject` (поле `Value` структуры `Base64Signature`).

### 3.3.10.6 Создание ЭП документа в формате Office Open XML

Для этого необходимо задать поле `SignatureType` равным `OOXML`.

Подписываемый документ в формате Office Open XML (`.docx`, `.xlsx`) должен быть указан в поле `InputDocument` (поле `Base64Data` структуры `Document`).

Свойства электронной подписи должны быть заданы в поле `OOXMLSignParameters` структуры `SignParameters` (см. Таблица 67).

Документ в формате Office Open XML с электронной подписью при успешном результате выполнения операции возвращается в поле `SignatureObject` (поле `Value` структуры `Base64Signature`).

### 3.3.11. Метод `verify`

Данный метод предназначен для проверки ЭП, а также для создания усовершенствованной ЭП (путём добавления метки доверенного времени).

Параметры:

- `verifyRequest` – структура `VerifyRequest` (см. Таблица 75).

Таблица 75 Описание полей структуры `VerifyRequest`

Поле	Тип	Описание
<code>InputDocument</code>	<code>InputDocumentType</code>	Подписанные данные (см. Таблица 45).
<code>SignatureObject</code>	<code>SignatureObjectType</code>	Объект подписи (см. Таблица 71).
<code>ReturnSigningTimeInfo</code>	<code>Object</code>	Если задано, в ответ сервера

		необходимо включить информацию о дате создания подписи и (если возможно) об интервале действительности подписи.
ReturnUpdatedSignature	ReturnUpdatedSignatureType	Если задано, необходимо усовершенствование ЭП, например, формирование долговременной подписи (см. Таблица 76). Подробнее см. п. 3.3.11.3.
ReturnTimestampedSignature	Object	Если задано, после проверки ЭП необходимо добавить в нее метку доверенного времени. Подробнее см. п. 3.3.11.2.
ReturnVerificationReport	Object	Если задано, в ответ сервера необходимо включить отчет о проверке - подробную информацию о результатах проверки ЭП.
SignatureType	String	Тип ЭП. Может принимать следующие значения: CMS - ЭП в формате CMS (по умолчанию), см. [2]; XMLDSIG - ЭП в формате XMLDSig (см. [4]); PADES – ЭП в формате PAdES [31]; OOXML – ЭП в формате OOXML [32].

Таблица 76 Описание полей структуры ReturnUpdatedSignatureType

Поле	Тип	Описание
Type	String	Тип возвращаемой подписи. Может принимать следующие значения: "urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T" "urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X" "urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L" "http://www.signal-com.ru/dss#detachedSignature"

Возвращаемое значение: структура VerifyResponse (см. Таблица 77).

Таблица 77 Описание полей структуры VerifyResponse

Поле	Тип	Описание
SigningTimeInfo	SigningTimeInfoType	Информация о дате создания подписи, а также об интервале действительности подписи (см. Таблица 78).
UpdatedSignature	UpdatedSignatureType	Усовершенствованная ЭП в формате CAdES (см. Таблица 80). Подробнее

		см. п. 3.3.11.3.
TimestampedSignature	TimestampedSignatureType	ЭП с добавленной меткой доверенного времени (см. Таблица 81). Подробнее см. п. 3.3.11.2.
VerificationReport	VerificationReportType	Отчет о проверке - подробная информация о результатах проверки ЭП (см. Таблица 82).
OutputDocument	DocumentType	Результирующий документ (см. Таблица 46).

Таблица 78 Описание полей структуры SigningTimeInfoType

Поле	Тип	Описание
SigningTime	DateTime	Информация о дате создания подписи. Извлекается из атрибута SigningTime подписи.
SigningTimeBoundaries	SigningTimeBoundaries	Информация об интервале действительности подписи (см. Таблица 79). Включается в ответ сервера только в случае, если подпись содержит метку доверенного времени.

Таблица 79 Описание полей структуры SigningTimeBoundaries

Поле	Тип	Описание
LowerBoundary	DateTime	Дата создания метки доверенного времени.
UpperBoundary	DateTime	Дата, до которой подпись может быть действительной.

Таблица 80 Описание полей структуры UpdatedSignatureType

Поле	Тип	Описание
Type	String	Тип возвращаемой подписи (см. Таблица 76).
SignatureObject	SignatureObjectType	Объект подписи (см. Таблица 71).

Таблица 81 Описание полей структуры TimestampedSignatureType

Поле	Тип	Описание
SignatureObject	SignatureObjectType	Объект подписи (см. Таблица 71).

Таблица 82 Описание полей структуры VerificationReportType

Поле	Тип	Описание
VerificationTime	DateTime	Дата проверки ЭП.
IndividualReport	List<IndividualReportType>	Список объектов IndividualReportType (см. Таблица 83).

Таблица 83 Описание полей структуры IndividualReportType

Поле	Тип	Описание
Valid	Boolean	True, если ЭП действительна.



Subject	String	Владелец сертификата ключа проверки ЭП в формате, соответствующем RFC 4514 [18].
Issuer	String	Издатель сертификата ключа проверки ЭП в формате, соответствующем RFC 4514 [18].
SerialNumber	Integer	Серийный номер сертификата ключа проверки ЭП.

### 3.3.11.1 Проверка ЭП в формате CMS

При выполнении операции проверки ЭП в формате CMS ее значение должно быть указано в поле SignatureObject.

При проверке отсоединённой (detached) ЭП подписанные данные должны быть указаны в элементе InputDocument.

### 3.3.11.2 Добавление метки доверенного времени к ЭП в формате CMS

Если Cloud DSS соответствующим образом сконфигурирован, он может после проверки ЭП добавить в нее метку доверенного времени.

Для этого необходимо включить в запрос поле ReturnTimestampedSignature.

Значения ЭП и подписанных данных кодируются как описано в п. 3.3.11.1.

Метки доверенного времени добавляется в ЭП как неподписанный атрибут с идентификатором 1.2.840.11359.1.9.16.2.14 согласно RFC 5126 [5].

При успешном выполнении операции поле TimestampedSignature в ответе сервера содержит ЭП с включённой меткой доверенного времени.

### 3.3.11.3 Создание усовершенствованной ЭП в формате CMS

Если Cloud DSS соответствующим образом сконфигурирован, он может после проверки ЭП при необходимости добавить в нее дополнительные атрибуты (в т. ч. метки доверенного времени).

Для этого необходимо задать поле ReturnUpdatedSignature с указанием типа возвращаемой ЭП в поле Type:

- urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-T;
- urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X;
- urn:oasis:names:tc:dss:1.0:profiles:AdES:forms:ES-X-L.

Значения ЭП, подлежащей проверке и модификации, а также подписанных данных кодируются как описано в п. 3.3.11.1.

ЭП, подлежащая модификации, должна иметь как минимум форму CAdES-BES, т. е. удовлетворять требованиям п. 4.3.1 [5]. При формировании ЭП типа ES-X или ES-X-L рекомендуется использовать в качестве исходной ЭП типа ES-T.

При успешном выполнении операции поле UpdatedSignature в ответе сервера содержит новое значение ЭП с дополнительными атрибутами (в т. ч. метки доверенного времени).

Если исходная ЭП уже имеет тип, указанный в запросе на модификацию, то производится только проверка ЭП, поле UpdatedSignature в этом случае в ответ не включается.

### 3.3.11.4 Проверка ЭП в формате XMLDSig

Для выполнения операции проверки ЭП XML-документ, содержащий одну или несколько подписей в формате XMLDSig, должен быть указан в элементе InputDocument. При этом производится проверка всех подписей, содержащихся в документе.

Для выборочной проверки подписей дополнительно необходимо задать поле SignatureObject, которое должно содержать поле SignaturePtr с атрибутом XPath, описывающим проверяемые ЭП [6].

### 3.3.11.5 Проверка ЭП документа в формате PDF

Для этого необходимо задать поле SignatureType равным PADES.

При выполнении операции проверки подписи документа в формате PDF документ должен быть указан в поле InputDocument (поле Base64Data структуры Document). При этом производится проверка всех электронных подписей, содержащихся в документе.

### 3.3.11.6 Проверка ЭП документа в формате Office Open XML

Для этого необходимо задать поле SignatureType равным OOXML.

При выполнении операции проверки подписи документа в формате Office Open XML документ должен быть указан в поле InputDocument (поле Base64Data структуры Document). При этом производится проверка всех электронных подписей, содержащихся в документе.

### 3.3.11.7 Удаление ЭП из документа в формате PDF

Для этого необходимо задать поле SignatureType равным PADES.

При выполнении операции удаления электронных подписей из документа в формате PDF используется метод verify. При этом в структуре ReturnUpdatedSignature (см. Таблица 76) должно быть задано поле Type, равное:

"http://www.signal-com.ru/dss#detachedSignature"

Исходный документ с электронными подписями должен быть указан в поле InputDocument (поле Base64Data структуры Document).

При успешном выполнении операции поле Base64Data структуры OutputDocument содержит документ в формате PDF без электронных подписей.

### 3.3.12. Метод getUserInfo

Данный метод предназначен для получения информации о текущем пользователе Cloud DSS.

Параметры:

- getUserInfoRequest – структура GetUserInfoRequest (см. п. 3.1.1).

Возвращаемое значение: структура GetUserInfoResponse (см. Таблица 84).

Таблица 84 Описание полей структуры GetUserInfoResponse

Поле	Тип	Описание
UserInfo	UserInfoType	Информация о текущем пользователе.

Таблица 85 Описание полей структуры UserInfoType

Поле	Тип	Описание
InternalSubject	InternalSubjectType	Параметры учетной записи пользователя (см. Таблица 86).
Role	String	Роль пользователя на сервере Cloud DSS. Может принимать следующие значения: CUSTOMER – пользователь; OPERATOR – оператор;

		ADMINISTRATOR – администратор.
DisplayName	String	Отображаемое имя пользователя.
Locked	Boolean	True, если учетная запись заблокирована.
CreationDate	DateTime	Дата создания учетной записи.
LastLoginDate	DateTime	Дата последнего входа.
PhoneNumber	String	Телефонный номер.
Email	String	Адрес электронной почты.
AuthenticationMethod	String	Метод вторичной аутентификации. Может принимать следующие значения:  OTP_VIA_SMS – отправка OTP в SMS;  OTP_VIA_EMAIL – отправка OTP с помощью электронной почты;  TOTP – протокол TOTP [24];  HOTP – протокол HOTP [25].
ConfirmedActions	UserActionListType	Список подтверждаемых операций (см. Таблица 87).
UserLocale	LocaleType	Информация о стране и языке (см. Таблица 88).
Transliteration	Boolean	True, если требуется транслитерация в SMS.
OTPClient	Integer	Идентификатор OTP-клиента. Используется, если задан метод вторичной аутентификации TOTP или HOTP.
SubjectAttributes	List<X509NameAttributeType>	Атрибуты имени пользователя в сертификате. Список объектов X509NameAttributeType (см. Таблица 111).
NotificationTransports	List<String>	Службы оповещений.

Таблица 86 Описание полей структуры InternalSubjectType

Поле	Тип	Описание
Login	String	Имя учетной записи.
ToBeChanged	Boolean	True, если пароль должен быть изменен.

Таблица 87 Описание полей структуры UserActionListType

Поле	Тип	Описание
Action	List<String>	Список подтверждаемых операций. Операция может принимать следующие значения:  LOGIN – вход;  CHANGE_PASSWORD – смена пароля;  GENERATE_CERTIFICATION_REQUEST – формирование запроса на создание сертификата ключа проверки ЭП;  SIGN – формирование ЭП;  CHANGE_PIN – смена PIN-кода виртуального

		токена; RENEW_CERTIFICATE – обновление сертификата; REVOKE_CERTIFICATE – аннулирование сертификата; DELETE_KEY_ENTRY – удаление ключа ЭП.
--	--	--

Таблица 88 Описание полей структуры LocaleType

Поле	Тип	Описание
Country	String	Код страны (ISO 3166 alpha-2).
Language	String	Код языка (ISO 639 alpha-2 или alpha-3).

### 3.3.13. Метод updateUserInfo

Данный метод предназначен для смены пароля пользователя.

Для этого необходимо в поле InternalSubject (см. Таблица 85) входных параметров задать значение ToBeChanged равным true. После вызова данного метода необходимо выполнить на сервере идентификации процедуру завершения сессии (см. п. 6.1.7), а затем процедуру получения маркера доступа (см. п. 6.1), в процессе которой пользователь будет перенаправлен на страницу сервера идентификации для ввода нового пароля.

Параметры:

- updateUserInfoRequest – структура UpdateUserInfoRequest (см. Таблица 89).

Таблица 89 Описание полей структуры UpdateUserInfoRequest

Поле	Тип	Описание
UserInfo	UserInfoType	Информация пользователя (см. Таблица 85) с параметром ToBeChanged равным true (см. Таблица 86).

Возвращаемое значение: структура UpdateUserInfoResponse (см. п. 3.1.2).

### 3.3.14. Метод encrypt

Данный метод предназначен для зашифрования данных в формате CMS.

Параметры:

- encryptRequest – структура EncryptRequest (см. Таблица 90).

Таблица 90 Описание полей структуры EncryptRequest

Поле	Тип	Описание
InputDocument	InputDocumentType	Данные, подлежащие зашифрованию (см. Таблица 45), должны быть указаны в поле Document.
EncryptionType	String	Формат зашифрованных данных. Может принимать следующие значения:  CMS - формат CMS (по умолчанию), см. [2].
ContentEncryptionMethod	ContentEncryptionMethodType	Параметры (алгоритм) шифрования (см. Таблица 91).

RecipientKeySelector	KeyInfoType	Параметры (сертификаты) получателей зашифрованных данных (см. [4]).
----------------------	-------------	---

Таблица 91 Описание полей структуры ContentEncryptionMethodType

Поле	Тип	Описание
Algorithm	String	Идентификатор алгоритма шифрования. Задается в соответствии с правилами RFC 3061, может принимать следующие значения:  "urn:oid:1.2.643.2.2.21" - алгоритм ГОСТ 28147-89 [30] в режиме гаммирования с обратной связью (по умолчанию).

Возвращаемое значение: структура EncryptResponse (см. Таблица 92).

Таблица 92 Описание полей структуры EncryptResponse

Поле	Тип	Описание
OutputDocument	DocumentType	Зашифрованные данные (см. Таблица 46).

### 3.3.15. Метод decrypt

Данный метод предназначен для расшифрования данных в формате CMS.

Параметры:

- decryptRequest – структура DecryptRequest (см. Таблица 93).

Таблица 93 Описание полей структуры DecryptRequest

Поле	Тип	Описание
InputDocument	InputDocumentType	Данные, подлежащие расшифрованию (см. Таблица 45), должны быть указаны в поле Document. Атрибут MimeType поля Base64Data (см. Таблица 47) должен быть установлен в значение «application/pkcs7-mime; smime-type=enveloped-data». Зашифрованные данные должны быть представлены в виде ASN.1 структуры ContentInfo с содержимым EnvelopedData [2].
EncryptionType	String	Формат зашифрованных данных. Может принимать следующие значения:  CMS - формат CMS (по умолчанию), см. [2].

Возвращаемое значение: структура DecryptResponse (см. Таблица 94).

Таблица 94 Описание полей структуры DecryptResponse

Поле	Тип	Описание
OutputDocument	DocumentType	Расшифрованные данные (см. Таблица 46).

### 3.3.16. Метод getGroupInfo

Данный метод предназначен для получения информации о группе пользователя.

Параметры:

- getGroupInfoRequest – структура GetGroupInfoRequest (см. п. 3.1.1).

Возвращаемое значение: структура GetGroupInfoResponse (см. Таблица 95).

Таблица 95 Описание полей структуры GetGroupInfoResponse

Поле	Тип	Описание
GroupInfo	GroupInfoType	Информация о группе пользователя (см. Таблица 101).

## 3.4. Интерфейс оператора

Описание интерфейса SOAP веб-сервиса оператора доступно по адресу:

[http://hostname\[:port\]/dss-operator-api/DSSOperatorWebService?wsdl](http://hostname[:port]/dss-operator-api/DSSOperatorWebService?wsdl)

hostname – адрес (IP или доменное имя) сервера приложений;

port – порт сервера приложений;

dss-operator-api – контекст веб-сервиса на сервере приложений.

Описание интерфейса REST веб-сервиса оператора доступно по адресу:

[http://hostname\[:port\]/dss-operator-api/rest/application.wadl](http://hostname[:port]/dss-operator-api/rest/application.wadl)

### 3.4.1. Метод getCAInfo

Данный метод предназначен для получения информации об Удостоверяющих центрах, зарегистрированных для групп оператора.

Параметры:

- getCAInfoRequest – структура GetCAInfoRequest (см. Таблица 96).

Таблица 96 Описание полей структуры GetCAInfoRequest

Поле	Тип	Описание
CA_ID	Integer	Идентификатор УЦ, по которому запрашивается информация. Если не задан, запрашивается информация по всем УЦ.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Возвращаемое значение: структура GetCAInfoResponse (см. Таблица 97).

Таблица 97 Описание полей структуры GetCAInfoResponse

Поле	Тип	Описание
CAs	CAInfoListType	Список параметров удостоверяющих центров (см. Таблица 9).

### 3.4.2. Метод getGroupInfo

Данный метод предназначен для получения информации о группах пользователей оператора.

Параметры:

- getGroupInfoRequest – структура GetGroupInfoRequest (см. Таблица 98).

Таблица 98 Описание полей структуры GetGroupInfoRequest

Поле	Тип	Описание
GroupID	Integer	Идентификатор группы, по которой запрашивается информация. Если идентификатор не задан, запрашивается информация по всем группам оператора.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Возвращаемое значение: структура GetGroupInfoResponse (см. Таблица 99).

Таблица 99 Описание полей структуры GetGroupInfoResponse

Поле	Тип	Описание
Groups	GroupInfoListType	Параметры групп (см. Таблица 100).

Таблица 100 Описание полей структуры GroupInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество групп.
Group	List<GroupInfoType>	Список объектов GroupInfoType (см. Таблица 101).

Таблица 101 Описание полей структуры GroupInfoType

Поле	Тип	Описание
GroupID	Integer	Идентификатор группы.
DisplayName	String	Отображаемое название группы.

AssignedCAs	CA_IDListType	Список УЦ группы (см. Таблица 102).
Operators	OperatorIDListType	Список операторов группы (см. Таблица 103).
Locked	Boolean	True, если группа заблокирована.
CreationDate	DateTime	Дата создания группы.
AuthenticationMethod	String	Метод вторичной аутентификации (см. Таблица 85). Используется для всех пользователей группы в случае, если AllowAuthenticationPolicyOverride равен false.
AllowAuthenticationPolicyOverride	Boolean	Если равен true, поле AuthenticationMethod игнорируется.
ConfirmedActions	UserActionListType	Список подтверждаемых операций (см. Таблица 87). Используется для всех пользователей группы в случае, если AllowConfirmationPolicyOverride равен false.
AllowConfirmationPolicyOverride	Boolean	Если равен true, поле ConfirmedActions игнорируется.
TSPServer	Integer	Идентификатор сервера меток доверенного времени.
NotificationTransports	List<String>	Службы оповещений.
AllowNotificationPolicyOverride	Boolean	Если равен true, поле NotificationTransports игнорируется.

Таблица 102 Описание полей структуры CA\_IDListType

Поле	Тип	Описание
CA_ID	List<Integer>	Список идентификаторов УЦ

Таблица 103 Описание полей структуры OperatorIDListType

Поле	Тип	Описание
OperatorID	List<Integer>	Список идентификаторов операторов.

### 3.4.3. Метод getOtpClientInfo

Данный метод предназначен для получения информации о параметрах OTP-клиентов, зарегистрированных в Cloud DSS. OTP-клиенты используются в протоколах TOTP [24] и HOTP [25] для вторичной аутентификации.

Параметры:

- getOtpClientInfoRequest – структура GetOtpClientInfoRequest (см. Таблица 104).



Таблица 104 Описание полей структуры GetOtpClientInfoRequest

Поле	Тип	Описание
OtpClientID	Integer	Идентификатор OTP-клиента. Если идентификатор не задан, запрашивается информация по всем OTP-клиентам.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Возвращаемое значение: структура GetOtpClientInfoResponse (см. Таблица 105).

Таблица 105 Описание полей структуры GetOtpClientInfoResponse

Поле	Тип	Описание
OtpClients	OtpClientInfoListType	Параметры OTP-клиентов (см. Таблица 106).

Таблица 106 Описание полей структуры OtpClientInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество OTP-клиентов.
OtpClient	List< OtpClientInfoType >	Список объектов OtpClientInfoType (см. Таблица 107).

Таблица 107 Описание полей структуры OtpClientInfoType

Поле	Тип	Описание
OtpClientID	Integer	Идентификатор OTP-клиента.
DisplayName	String	Отображаемое название OTP-клиента.
AuthenticationMethod	String	Метод вторичной аутентификации. Может принимать следующие значения: TOTP – протокол TOTP; HOTP – протокол HOTP.
HMACHashAlgorithm	String	Идентификатор HMAC-алгоритма. Задается в соответствии с правилами RFC 3061, может принимать следующие значения: "urn:oid:1.2.840.113549.2.7" – алгоритм HMAC-SHA1; "urn:oid:1.2.840.113549.2.9" – алгоритм HMAC-SHA256;

		"urn:oid:1.2.840.113549.2.10" – алгоритм HMAC-SHA384; "urn:oid:1.2.840.113549.2.11" – алгоритм HMAC-SHA512; "urn:oid:1.2.643.7.1.1.4.1" – алгоритм HMAC-GOSTR3411-2012-256; "urn:oid:1.2.643.7.1.1.4.2" – алгоритм HMAC-GOSTR3411-2012-512.
PSKLength	Integer	Длина разделяемого секрета.
Digits	Integer	Количество десятичных знаков в OTP.
Throttle	Integer	Порог блокировки учетной записи.
Resynch	Integer	Look-ahead window - для HOTP, time steps - для TOTP
Properties	List<PropertyType>	Дополнительные параметры. Список объектов PropertyType (см. Таблица 108).
Locked	Boolean	True, если OTP-клиент заблокирован.
CreationDate	DateTime	Дата создания OTP-клиента.

Таблица 108 Описание полей структуры PropertyType

Поле	Тип	Описание
key	String	Имя параметра.
value	String	Значение параметра.

### 3.4.4. Метод addCustomer

Данный метод предназначен для добавления нового пользователя Cloud DSS.

Параметры:

- addCustomerRequest – структура AddCustomerRequest (см. Таблица 109).

Таблица 109 Описание полей структуры AddCustomerRequest

Поле	Тип	Описание
CustomerInfo	CustomerInfoType	Информация пользователя (см. Таблица 110).

Таблица 110 Описание полей структуры CustomerInfoType

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя. В методе addCustomer не используется.
InternalSubject	InternalSubjectType	Параметры учетной записи (см. Таблица 86). В данной операции не используется.
Group	Integer	Идентификатор группы (см. п. 3.4.2).

DisplayName	String	Отображаемое имя.
Locked	Boolean	True, если учетная запись заблокирована.
CreationDate	DateTime	Дата создания учетной записи.
LastLoginDate	DateTime	Дата последнего входа.
PhoneNumber	String	Телефонный номер.
PhoneConfirmed	Boolean	True, если номер телефона был подтвержден (см. п. 3.4.16).
Email	String	Адрес электронной почты.
EmailConfirmed	Boolean	True, если адрес электронной почты был подтвержден (см. п. 3.4.16).
AuthenticationMethod	String	Метод вторичной аутентификации (см. Таблица 85).
ConfirmedActions	UserActionListType	Список подтверждаемых операций (см. Таблица 87).
UserLocale	LocaleType	Информация о стране и языке (см. Таблица 88).
Transliteration	Boolean	True, если требуется транслитерация в SMS.
OTPClient	Integer	Идентификатор OTP-клиента. Используется, если задан метод вторичной аутентификации TOTP или HOTP (см. п. 3.4.3).
SubjectAttributes	List<X509NameAttributeType>	Атрибуты имени пользователя в сертификате. Список объектов X509NameAttributeType (см. Таблица 111).
NotificationTransports	List<String>	Службы оповещений.

Таблица 111 Описание полей структуры X509NameAttributeType

Поле	Тип	Описание
oid	String	Стандартный идентификатор атрибута имени в соответствии с правилами RFC 3061, например: "urn:oid:2.5.4.6" – countryName; "urn:oid:2.5.4.7" – localityName; "urn:oid:2.5.4.9" – streetAddress; "urn:oid:2.5.4.10" – organizationName.
value	String	Значение атрибута.

Возвращаемое значение: структура AddCustomerResponse (см. Таблица 112).

Таблица 112 Описание полей структуры AddCustomerResponse

Поле	Тип	Описание
------	-----	----------

CustomerID	Integer	Идентификатор пользователя.
InternalSubject	InternalSubjectType	Параметры учетной записи (см. Таблица 86).
Password	String	Пароль.

### 3.4.5. Метод getCustomerInfo

Данный метод предназначен для получения информации о пользователях Cloud DSS.

Параметры:

- getCustomerInfoRequest – структура GetCustomerInfoRequest (см. Таблица 113).

Таблица 113 Описание полей структуры GetCustomerInfoRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя, по которому запрашивается информация. Если идентификатор не задан, запрашивается информация по всем пользователям.
ObjectFilter	ObjectFilterType	Фильтр объектов. Может быть операцией сравнения или логической операцией (см. Таблица 114). Допустимые поля фильтра для данной структуры см. Таблица 117.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Таблица 114 Описание полей структуры ObjectFilterType

Поле	Тип	Описание
Field	ObjectFieldType	Операция сравнения (см. Таблица 115).
Condition	ObjectConditionType	Логическая операция (см. Таблица 116).

Таблица 115 Описание полей структуры ObjectFieldType

Поле	Тип	Описание
Operator	String	Тип операции сравнения: EQUAL – равно; NOT_EQUAL – не равно; LIKE – подобие; GREATER – больше; LESS – меньше.
Name	String	Имя поля объекта, к которому применяется операция сравнения.
Value	Object	Сравниваемое значение.

Таблица 116 Описание полей структуры ObjectConditionType

Поле	Тип	Описание
------	-----	----------

Operator	String	Тип логической операции: AND – «И»; OR – «ИЛИ»; NOT – «НЕТ».
FieldOrCondition	List<Object>	Список операций, к которым применяется логическая операция: классы ObjectFieldType и ObjectConditionType.

Таблица 117 Допустимые поля фильтра объектов структуры GetCustomerInfoRequest

Поле	Тип	Описание
groupId	Integer	Идентификатор группы пользователей.
search	String	Подстрока атрибута имени пользователя.

Возвращаемое значение: структура GetCustomerInfoResponse (см. Таблица 118).

Таблица 118 Описание полей структуры GetCustomerInfoResponse

Поле	Тип	Описание
Customers	CustomerInfoListType	Параметры пользователей (см. Таблица 119).

Таблица 119 Описание полей структуры CustomerInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество пользователей.
Customer	List<CustomerInfoType>	Список объектов CustomerInfoType (см. Таблица 110).

### 3.4.6. Метод updateCustomerInfo

Данный метод предназначен для изменения информации пользователя.

Параметры:

- updateCustomerInfoRequest – структура UpdateCustomerInfoRequest (см. Таблица 120).

Таблица 120 Описание полей структуры UpdateCustomerInfoRequest

Поле	Тип	Описание
CustomerInfo	CustomerInfoType	Информация пользователя (см. Таблица 110).

Возвращаемое значение: структура UpdateCustomerInfoResponse (см. п. 3.1.2).

### 3.4.7. Метод deleteCustomer

Данный метод предназначен для удаления учетной записи пользователя Cloud DSS.

Параметры:

- deleteCustomerRequest – структура DeleteCustomerRequest (см. Таблица 121).

Таблица 121 Описание полей структуры DeleteCustomerRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.

Возвращаемое значение: структура DeleteCustomerResponse (см. п. 3.1.2).

### 3.4.8. Метод getCustomerKeyEntryInfo

Данный метод предназначен для получения информации о ключах ЭП, запросах на создание сертификатов ключей проверки ЭП, сертификатах ключей проверки ЭП и запросах на аннулирование сертификатов ключей проверки ЭП заданного пользователя.

Перед выдачей этой информации выполняется обращение к веб-сервису Удостоверяющего центра для получения актуальных статусов объектов и загрузки созданных сертификатов ключей проверки ЭП.

Параметры:

- getCustomerKeyEntryInfoRequest – структура GetCustomerKeyEntryInfoRequest (см. Таблица 122).

Таблица 122 Описание полей структуры GetCustomerKeyEntryInfoRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя, по которому запрашивается информация.
KeySelector	KeySelectorType	Идентификатор ключа ЭП (см. п. 3.1.3). Если поле не задано, выдается информация для всех ключей ЭП пользователя.
ResultFormat	String	Формат кодирования получаемых параметров (запросов на создание сертификата и сертификатов ключей проверки ЭП): "ASN.1" – формат ASN.1 (используется по умолчанию); "PEM" – формат PEM.

Возвращаемое значение: структура GetCustomerKeyEntryInfoResponse (см. Таблица 123).

Таблица 123 Описание полей структуры GetCustomerKeyEntryInfoResponse

Поле	Тип	Описание
KeyEntries	KeyEntryInfoListType	Параметры ключей ЭП (см. Таблица 124).

Таблица 124 Описание полей структуры KeyEntryInfoListType

Поле	Тип	Описание
TotalNumber	Integer	Общее количество ключей ЭП.
KeyEntry	List<KeyEntryInfoType>	Список объектов KeyEntryInfoType (см. Таблица 32).

### 3.4.9. Метод generateCustomerCMC

Данный метод предназначен для подписания запроса на создание сертификата ключа проверки ЭП пользователя в формате PKCS #10 [7] ключом ЭП оператора (формирование запроса в формате СМС [8]).

В случае успешного завершения операции сформированный запрос на создание сертификата ключа проверки ЭП пользователя в формате СМС автоматически отправляется в Удостоверяющий центр. В дальнейшем можно проверить статус обработки запроса на создание

сертификата ключа проверки ЭП и загрузить изготовленный Удостоверяющим центром сертификат ключа проверки ЭП (см. п.п. 3.4.8 и 3.4.15).

Параметры:

- generateCustomerCMCRequest – структура GenerateCustomerCMCRequest (см. Таблица 125).

Таблица 125 Описание полей структуры GenerateCustomerCMCRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.
KeySelector	KeySelectorType	Идентификатор ключа ЭП пользователя (см. п. 3.1.3).
SignatureKey	KeySelectorType	Идентификатор ключа ЭП оператора для подписи СМС-запроса.
AddSignerCertificate	Boolean	Управляет включением сертификата ключа проверки ЭП в ЭП СМС-запроса (по умолчанию сертификат включается).

Возвращаемое значение: структура GenerateCustomerCMCResponse (см. п. 3.1.2).

### 3.4.10. Метод updateCustomerKeyEntryInfo

Данный метод предназначен для выполнения одной из следующих операций: аннулирование сертификата ключа проверки ЭП пользователя Cloud DSS, приостановка действия его сертификата, возобновление действия сертификата пользователя.

Параметры:

- updateCustomerKeyEntryInfoRequest – структура UpdateCustomerKeyEntryInfoRequest (см. Таблица 126).

Таблица 126 Описание полей структуры UpdateCustomerKeyEntryInfoRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.
KeySelector	KeySelectorType	Идентификатор ключа ЭП пользователя (см. п. 3.1.3).
SignatureKey	KeySelectorType	Идентификатор ключа ЭП оператора для подписи СМС-запроса.
UpdatedKeyEntryInfo	UpdatedKeyEntryInfoType	Изменяемые параметры ключа ЭП пользователя (см. Таблица 127).

Таблица 127 Описание полей структуры UpdatedKeyEntryInfoType

Поле	Тип	Описание
X509CertificateStatus	X509CertificateStatusType	Информация о статусе сертификата ключа проверки ЭП пользователя (см. Таблица 35).

Возвращаемое значение: структура UpdateCustomerKeyEntryInfoResponse (см. п. 3.1.2).

### 3.4.11. Метод getCustomerTokenInfo

Данный метод предназначен для получения информации о виртуальном токене пользователя Cloud DSS.

Параметры:

- `getCustomerTokenInfoRequest` – структура `GetCustomerTokenInfoRequest` (см. Таблица 128).

Таблица 128 Описание полей структуры `GetCustomerTokenInfoRequest`

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.

Возвращаемое значение: структура `GetCustomerTokenInfoResponse` (см. Таблица 129).

Таблица 129 Описание полей структуры `GetCustomerTokenInfoResponse`

Поле	Тип	Описание
TokenInfo	TokenInfoType	Параметры виртуального токена (см. Таблица 42).

### 3.4.12. Метод `updateCustomerTokenInfo`

Данный метод предназначен для изменения параметров виртуального токена пользователя Cloud DSS.

Параметры:

- `updateCustomerTokenInfoRequest` – структура `UpdateCustomerTokenInfoRequest` (см. Таблица 130).

Таблица 130 Описание полей структуры `UpdateCustomerTokenInfoRequest`

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.
TokenInfo	TokenInfoType	Изменяемые параметры виртуального токена пользователя (см. Таблица 42).

Возвращаемое значение: структура `UpdateCustomerTokenInfoResponse` (см. п. 3.1.2).

### 3.4.13. Метод `getUserInfo`

Данный метод предназначен для получения информации о текущем операторе.

Параметры:

- `getUserInfoRequest` – структура `GetUserInfoRequest` (см. п. 3.1.1).

Возвращаемое значение: структура `GetUserInfoResponse` (см. Таблица 131).

Таблица 131 Описание полей структуры `GetUserInfoResponse`

Поле	Тип	Описание
UserInfo	UserInfoType	Информация оператора (см. Таблица 85).

### 3.4.14. Метод `updateUserInfo`

Данный метод предназначен для смены пароля оператора.

Для этого необходимо в поле `InternalSubject` (см. Таблица 85) входных параметров задать значение `ToBeChanged` равным `true`. После вызова данного метода необходимо выполнить на сервере идентификации процедуру завершения сессии (см. п. 6.1.7), а затем процедуру



получения маркера доступа (см. п. 6.1), в процессе которой оператор будет перенаправлен на страницу сервера идентификации для ввода нового пароля.

Параметры:

- updateUserInfoRequest – структура UpdateUserInfoRequest (см. Таблица 132).

Таблица 132 Описание полей UpdateUserInfoRequest

Поле	Тип	Описание
UserInfo	UserInfoType	Информация оператора (см. Таблица 85) с параметром ToBeChanged равным true (см. Таблица 86).

Возвращаемое значение: структура UpdateUserInfoResponse (см. п. 3.1.2).

### 3.4.15. Метод getCustomerObjects

Данный метод предназначен для получения информации о запросах на создание сертификатов ключей проверки ЭП, сертификатах ключей проверки ЭП или запросах на аннулирование сертификатов ключей проверки ЭП всех пользователей данного оператора или отдельной группы пользователей.

Перед выдачей этой информации выполняется обращение к веб-сервису Удостоверяющего центра для получения актуальных статусов объектов и загрузки созданных сертификатов ключей проверки ЭП.

Параметры:

- getCustomerObjectsRequest – структура GetCustomerObjectsRequest (см. Таблица 133).

Таблица 133 Описание полей структуры GetCustomerObjectsRequest

Поле	Тип	Описание
ObjectType	String	Тип объекта в списке. Может принимать следующие значения:  CertificationRequest – запрос на создание сертификата;  X509Certificate – сертификат;  RevocationRequest – запрос на аннулирование сертификата.
ObjectFilter	ObjectFilterType	Фильтр объектов (см. Таблица 114). Допустимые поля фильтра для данной структуры см. Таблица 134.
ResultFormat	String	Формат кодирования получаемых объектов:  "ASN.1" – формат ASN.1 (используется по умолчанию);  "PEM" – формат PEM.
First	Integer	Номер первого объекта в списке.
Count	Integer	Максимальное количество объектов в списке. Если значение меньше нуля, возвращается полный список. Если значение равно нулю, возвращается только общее количество объектов.

Таблица 134 Допустимые поля фильтра объектов структуры GetCustomerObjectsRequest

Поле	Тип	Описание
groupId	Integer	Идентификатор группы пользователей.

Возвращаемое значение: структура GetCustomerObjectsResponse (см. Таблица 135).

Таблица 135 Описание полей структуры GetCustomerObjectsResponse

Поле	Тип	Описание
X509Certificates	X509CertificateListType	Список сертификатов (см. Таблица 136).
CertificationRequests	CertificationRequestListType	Список запросов на создание сертификата (см. Таблица 137).
RevocationRequests	RevocationRequestListType	Список запросов на аннулирование сертификата (см. Таблица 138).

Таблица 136 Описание полей структуры X509CertificateListType

Поле	Тип	Описание
TotalNumber	Integer	Общее число сертификатов.
X509Certificate	List<X509CertificateType>	Список объектов X509CertificateType (см. Таблица 34).

Таблица 137 Описание полей структуры CertificationRequestListType

Поле	Тип	Описание
TotalNumber	Integer	Общее число запросов на создание сертификата.
CertificationRequest	List<CertificationRequestType>	Список объектов CertificationRequestType (см. Таблица 33).

Таблица 138 Описание полей структуры RevocationRequestListType

Поле	Тип	Описание
TotalNumber	Integer	Общее число запросов на аннулирование сертификата.
RevocationRequest	List<RevocationRequestType>	Список объектов RevocationRequestType (см. Таблица 37).

### 3.4.16. Метод confirmCustomerInfo

Данный метод предназначен для подтверждения телефонного номера или адреса электронной почты пользователя. Метод confirmCustomerInfo всегда выполняется в асинхронном режиме (см. п. 3.2).

Параметры:

- confirmCustomerInfoRequest – структура ConfirmCustomerInfoRequest (см. Таблица 139).

Таблица 139 Описание полей структуры ConfirmCustomerInfoRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.

ConfirmedInfo	String	Подтверждаемый параметр: " PhoneNumber" – телефонный номер; " Email" – адрес электронной почты.
---------------	--------	---

Возвращаемое значение: структура ConfirmCustomerInfoResponse (см. п. 3.1.2).

### 3.4.17. Метод getCustomerPSK

Данный метод предназначен для получения разделяемого секрета пользователя в виде строки в формате Base32 и QR-кода (опционально).

Разделяемый секрет используется в протоколах TOTP [24] и HOTP [25] для вторичной аутентификации.

Данная информация является конфиденциальной и передается пользователю при личной встрече (например, при регистрации в Cloud DSS) для задания (сканирования) в OTP-клиентах (приложениях) пользователя.

Параметры:

- getCustomerPSKRequest – структура GetCustomerPSKRequest (см. Таблица 140).

Таблица 140 Описание полей структуры GetCustomerPSKRequest

Поле	Тип	Описание
CustomerID	Integer	Идентификатор пользователя.
QRCodeImageInfo	QRCodeImageInfoType	Параметры QR-кода (см. Таблица 141).

Таблица 141 Описание полей структуры QRCodeImageInfoType

Поле	Тип	Описание
Format	String	Формат QR-кода, может принимать следующие значения: "PNG", "JPEG" и "GIF".
Width	Integer	Ширина QR-кода в пикселях.
Height	Integer	Высота QR-кода в пикселях.

Возвращаемое значение: структура GetCustomerPSKResponse (см. Таблица 142).

Таблица 142 Описание полей структуры GetCustomerPSKResponse

Поле	Тип	Описание
Base32Secret	byte[]	Разделяемый секрет в формате Base32.
QRCodeImage	byte[]	QR-код разделяемого секрета.

#### **4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ**

Входные и выходные данные, используемые в интерфейсах веб-сервисов Cloud DSS, задаются в виде структур (классов), базовые типы которых описаны в п. 3.1.

## 5. СООБЩЕНИЯ

Сообщения о результатах обращения к методам веб-сервисов Cloud DSS содержатся в структуре Result (п. 3.1.2).

Список значений поля ResultMinor для веб-сервиса пользователя и веб-сервиса оператора приведены в Таблица 143 и Таблица 144.

Таблица 143 Список значений ResultMinor для веб-сервиса пользователя

Значение	Описание
ConfirmationRequired	Требуется подтверждение транзакции.
OperationCompleted	Операция завершена.
GeneralError	Причина ошибки может быть определена с помощью журнала событий сервера Cloud DSS [20].
UnsupportedKeyAlgorithm	Заданный алгоритм ключей ЭП не поддерживается.
UnsupportedKeyParameters	Заданные параметры алгоритма ключей ЭП не поддерживаются.
InvalidKeySelector	Неверное задание структуры KeySelector.
UnsupportedKeySelector	Заданное в структуре KeySelector поле не поддерживается.
KeyNotFound	Ключ ЭП с заданным в структуре KeySelector идентификатором отсутствует.
InvalidSubjectType	Неверное задание структуры X509SubjectName.
UnsupportedSubjectType	Заданное в структуре X509SubjectName поле не поддерживается.
UnsupportedX509Extensions	Заданное в структуре X509Extensions поле не поддерживается.
InvalidSignatureKey	Неверное задание структуры SignatureKey.
UnsupportedSignatureKey	Заданное в структуре SignatureKey поле не поддерживается.
SignatureKeyNotFound	Ключ ЭП с заданным в структуре SignatureKey идентификатором отсутствует.
InvalidCertificate	Ошибка при декодировании сертификата ключа проверки ЭП.
InvalidAccessToken	Маркер доступа не задан или недействителен.
InvalidUserEntity	Неверный идентификатор пользователя.
InvalidTokenId	Виртуальный токен не назначен.
invalid:IncorrectSignature	Подпись недействительна.
valid:signature:InvalidSignatureTimestamp	Подпись действительна, однако метка доверенного времени для этой подписи недействителен.
KeyInfoNotProvided	Требуемая ключевая информация не была предоставлена.
InvalidRefURI	Недопустимое значение атрибута RefURI,

	включенного во входной документ.
NotParseableXMLDocument	Ошибка при разборе документа.
Inappropriate:signature	Подпись или ее содержимое не могут использоваться в текущем контексте.
invalid:KeyLookupFailed	Не удалось найти указанный ключ.
CrlNotAvailiable	Список аннулированных сертификатов не доступен.
OcspNotAvailiable	OCSP не доступен.
CertificateChainNotComplete	Невозможно построить цепочку сертификатов.
InvalidParameter	Параметр задан неверно.
InvalidTransactionID	Неверный идентификатор транзакции.
TransactionNotConfirmed	Операция не была подтверждена.
TransactionExpired	Время подтверждения транзакции истекло.
InvalidTransactionUser	Данная транзакция создана для другого пользователя.
InvalidTransactionRequest	Идентификатор транзакции не соответствует вызываемому методу.
DocumentNotSpecified	Документ для создания или проверки ЭП не задан.
UnsupportedSignatureType	Данный тип ЭП не поддерживается.
SignatureNotSpecified	Электронная подпись для проверки не задана.
DocumentNameTooLarge	Название документа (см. Таблица 45) превышает максимальное допустимое значение.
DocumentTooLarge	Размер документа превышает максимальное допустимое значение.
InvalidCaID	Неверный идентификатор Удостоверяющего центра.
InvalidTemplateID	Неверный идентификатор шаблона.
SubjectAttributeNotFound	Обязательный атрибут имени не найден.

Таблица 144 Список значений ResultMinor для веб-сервиса оператора

Значение	Описание
ConfirmationRequired	Требуется подтверждение транзакции.
OperationCompleted	Операция завершена.
GeneralError	Причина ошибки может быть определена с помощью журнала событий сервера Cloud DSS [20].
InvalidAccessToken	Маркер доступа не задан или недействителен.
InvalidUserEntity	Неверный идентификатор пользователя.
AccessDenied	Доступ к заданному объекту запрещен.
InvalidTokenId	Виртуальный токен не назначен.

InvalidKeySelector	Неверное задание структуры KeySelector.
UnsupportedKeySelector	Заданное в структуре KeySelector поле не поддерживается.
KeyNotFound	Ключ ЭП с заданным в структуре KeySelector идентификатором отсутствует.
InvalidSignatureKey	Неверное задание структуры SignatureKey.
UnsupportedSignatureKey	Заданное в структуре SignatureKey поле не поддерживается.
SignatureKeyNotFound	Ключ ЭП с заданным в структуре SignatureKey идентификатором отсутствует.
InvalidParameter	Параметр задан неверно.
InvalidTransactionID	Неверный идентификатор транзакции.
TransactionNotConfirmed	Операция не была подтверждена.
TransactionExpired	Время подтверждения транзакции истекло.
InvalidTransactionUser	Данная транзакция создана для другого пользователя.
InvalidTransactionRequest	Идентификатор транзакции не соответствует вызываемому методу.

## 6. АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И ПОЛУЧЕНИЕ МАРКЕРА ДОСТУПА

Для аутентификации пользователя, получения маркера доступа (см. п. 3), а также подтверждения операций пользователя (см. п. 3.2) в Cloud DSS используется сервер идентификации.

Для взаимодействия с сервером идентификации клиентское приложение может использовать протоколы OAuth 2.0 [22] и/или WS-Trust [26].

### 6.1. Протокол OAuth

Текущая реализация сервера идентификации поддерживает только сценарий аутентификации с кодом авторизации. Сценарий состоит из двух шагов: получение кода авторизации и получение маркера доступа.

#### 6.1.1. Получение кода авторизации

Для получения кода авторизации клиентское приложение (далее клиент) должно перенаправить пользователя на сервер идентификации, используя следующий GET HTTP-запрос:

`http://hostname[:port]/dss-identity-sp/idp/oauth/authorize?response_type=code&client_id=%CLIENT_ID%&redirect_uri=%REDIRECT_URI%&scope=%SCOPE%&state=%STATE%`

В запросе кода авторизации используются следующие параметры:

Параметр	Значение	Описание
response_type	'code'	Признак сценария с кодом авторизации
client_id	%CLIENT_ID%	Идентификатор клиентского приложения, зарегистрированный на сервере идентификации
redirect_uri	%REDIRECT_URI%	Адрес для возврата клиенту кода авторизации, зарегистрированный на сервере идентификации
Scope	%SCOPE%	Параметр зарезервирован для будущего использования, в текущей реализации игнорируется
State	%STATE%	Параметр используется клиентом OAuth 2.0 для проверки подлинности ответа от сервера

В ответ на запрос кода авторизации сервер идентификации перенаправляет пользователя на страницу(ы) аутентификации. В случае успешной аутентификации пользователя сервер идентификации перенаправляет его на адрес %REDIRECT\_URI%, возвращая код авторизации в следующем GET HTTP-запросе:

`%REDIRECT_URI%?code=%CODE%&state=%STATE%`

При возврате кода авторизации используются следующие параметры:

Параметр	Значение	Описание
code	%CODE%	Значение кода авторизации



state	%STATE%	Параметр используется клиентом OAuth 2.0 для проверки подлинности ответа от сервера
-------	---------	---

### 6.1.2. Получение маркера доступа

После получения кода авторизации клиент должен отправить серверу идентификации следующий POST HTTP-запрос:

`http://hostname[:port]/dss-identity-sp/api/token`

В теле запроса маркера доступа используются следующие параметры:

Параметр	Значение	Описание
grant_type	'authorization_code'	Признак сценария с кодом авторизации
code	%CODE%	Значение кода авторизации
redirect_uri	%REDIRECT_URI%	Адрес для возврата клиенту кода авторизации, зарегистрированный на сервере идентификации
client_id	%CLIENT_ID%	Идентификатор клиентского приложения, зарегистрированный на сервере идентификации
client_secret	%CLIENT_SECRET%	Пароль клиентского приложения, зарегистрированный на сервере идентификации

После успешной проверки запроса на получение маркера доступа сервер идентификации возвращает клиенту маркер доступа в следующем JSON-ответе:

`{"access_token": "%ACCESS_TOKEN%", "expires_in": "%EXPIRES_IN%"}`

В JSON-ответе с маркером доступа используются следующие параметры:

Параметр	Значение	Описание
access_token	%ACCESS_TOKEN%	Значение маркера доступа
expires_in	%EXPIRES_IN%	Время жизни маркера доступа в секундах

### 6.1.3. Подтверждение операции пользователя

Для подтверждения операции необходимо выполнить сценарий, аналогичный описанному в п. 6.1.1, с дополнительным параметром `transaction_id`, идентифицирующим операцию. Данный параметр возвращается при вызове метода веб-сервиса, если для выполнения этой операции требуется ее подтверждение пользователем (определяется настройками Cloud DSS, см. п. 3.2).

Для этого клиентское приложение должно перенаправить пользователя на сервер идентификации, используя следующий GET HTTP-запрос:

`http://hostname[:port]/dss-identity-sp/idp/oauth/authorize?response_type=code&client_id=%CLIENT_ID%&redirect_uri=%REDIRECT_URI%&scope=%SCOPE%&state=%STATE%&transaction_id=%TRANSACTION_ID%`

В запросе подтверждения операции пользователя используются следующие параметры:

Параметр	Значение	Описание
response_type	'code'	Признак сценария с кодом авторизации
client_id	%CLIENT_ID%	Идентификатор клиентского приложения, зарегистрированный на сервере идентификации
redirect_uri	%REDIRECT_URI%	Адрес для возврата клиенту кода авторизации, зарегистрированный на сервере идентификации
scope	%SCOPE%	Параметр зарезервирован для будущего использования, в текущей реализации игнорируется
state	%STATE%	Параметр используется клиентом OAuth 2.0 для проверки подлинности ответа от сервера
transaction_id	%TRANSACTION_ID%	Уникальный идентификатор транзакции при выполнении операции.

В ответ на этот запрос сервер идентификации перенаправляет пользователя на страницу подтверждения операции. В случае успешного подтверждения операции пользователем сервер идентификации перенаправляет его на адрес %REDIRECT\_URI%, возвращая код авторизации в следующем GET HTTP-запросе:

`%REDIRECT_URI%?code=%CODE%&state=%STATE%&error=%ERROR%&transaction_id=%TRANSACTION_ID%`

При возврате кода авторизации используются следующие параметры:

Параметр	Значение	Описание
code	%CODE%	Значение кода авторизации
state	%STATE%	Параметр используется клиентом OAuth 2.0 для проверки подлинности ответа от сервера
error	%ERROR%	Присутствует в случае ошибки выполнения запроса
transaction_id	%TRANSACTION_ID%	Уникальный идентификатор транзакции при выполнении операции.

При отсутствии параметра error (или пустом значении %ERROR%) запрос считается выполненным успешно, а операция пользователя с идентификатором transaction\_id считается подтвержденной.

После подтверждения операции необходимо для завершения операции и получения результата вызвать метод веб-сервиса повторно, задав тот же идентификатор транзакции (см. п. 3.2).

Если сессия браузера пользователя в сервисе идентификации к моменту подтверждения операции будет завершена, то перед возвратом кода авторизации пользователь будет перенаправлен на страницу(ы) аутентификации.

#### 6.1.4. Обновление маркера доступа

Если сессия браузера пользователя в сервисе идентификации не завершена, а время жизни текущего маркера доступа подходит к концу, маркер доступа можно обновить, выполнив сценарий, аналогичный описанному в п. 6.1.

При этом клиентское приложение получит новый маркер доступа без перенаправления пользователя на страницу(ы) аутентификации.

Если сессия браузера пользователя в сервисе идентификации к моменту обновления маркера доступа будет завершена, то в процессе получения нового маркера доступа пользователь будет перенаправлен на страницу(ы) аутентификации.

#### 6.1.5. Обновление маркера доступа при подтверждении операции пользователя

Если время жизни текущего маркера доступа подходит к концу, маркер доступа можно обновить, выполнив после сценария п. 6.2 , дополнительно сценарий, описанный в п. 6.1.2 для получения нового маркера доступа по коду авторизации.

#### 6.1.6. Использование стандартных клиентов OAuth 2.0

Сервер идентификации обеспечивает поддержку стандартных клиентов OAuth 2.0 при аутентификации пользователей по сценарию, описанному в п. 6.1.

Также для поддержки стандартных клиентов OAuth 2.0 сервер идентификации дополнительно реализует точку доступа для запроса информации о профиле пользователя следующим GET HTTP-запросом:

`http://hostname[:port]/dss-identity-sp/verify/token`

Запрос должен содержать маркер доступа в заголовке:

`“Authorization: Bearer %ACCESS_TOKEN%”`

После успешной проверки сервером идентификации маркера доступа сервер идентификации возвращает клиенту информацию о профиле пользователя в следующем JSON-ответе:

`{“dssUserId”:”%DSSUSERID%”}`

В JSON-ответе с информацией о профиле пользователя используются следующие параметры:

Параметр	Значение	Описание
dssUserId	%DSSUSERID%	Идентификатор пользователя сервера идентификации

#### 6.1.7. Завершение сессии пользователя на сервере идентификации (logout)

Для завершения сессии браузера пользователя на сервере идентификации клиентскому приложению необходимо выполнить перенаправление пользователя, используя GET HTTP-запрос, на следующий URL:

`http://hostname[:port]/dss-identity-sp/idp/oauth/logout? client_id= %CLIENT_ID%`

В запросе завершения сессии используются следующие параметры:

Параметр	Значение	Описание
client_id	%CLIENT_ID%	Идентификатор клиентского приложения, зарегистрированный на сервере идентификации

После завершения сессии пользователя сервер идентификации перенаправит пользователя, используя GET HTTP-запрос, на следующий URL: %LOGOUTURL%.

Этот URL задается в настройках клиентского приложения, зарегистрированного на сервере идентификации.

## 6.2. Протокол WS-Trust

В текущей реализации сервера идентификации Cloud DSS используется протокол WS-Trust 1.3 [26].

Первичная аутентификация пользователя в Security Token Service (STS) сервера идентификации выполняется в соответствии со спецификацией WS-Security [28].

Для этого используется маркер безопасности UsernameToken [29], который вставляется в элемент Security заголовка всех SOAP-сообщений пользователя. Пароль пользователя задается параметром типа #PasswordText.

Для вторичной аутентификации пользователя в STS используется расширение User Interaction Challenge (UIC) базового протокола WS-Trust 1.3, описанное в WS-Trust 1.4 [27].

Расширение UIC предназначено для получения от пользователя дополнительных параметров аутентификации в интерактивном режиме.

Взаимодействие с STS осуществляется по протоколу TLS.

### 6.2.1. Получение маркера доступа

Для получения маркера доступа (см. п. 3) пользователь посылает STS сообщение-запрос RequestSecurityToken (RST) следующего вида (см. Таблица 145):

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:c14n="http://www.w3.org/2001/10/xml-
exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml1="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xenc="http://www.w3.org/2001/04/xmenc#" xmlns:wsc="http://docs.oasis-open.org/ws-sx/ws-
secureconversation/200512" xmlns:sts="http://sts.dss.signalcom.ru/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:chan="http://schemas.microsoft.com/ws/2005/02/duplex"
xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:auth="http://docs.oasis-
open.org/wsfed/authorization/200706" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-
open.org/ws-sx/ws-trust/200802">
  <SOAP-ENV:Header>
    <wsse:Security SOAP-ENV:mustUnderstand="1">
      <wsse:UsernameToken wsu:Id="User">
        <wsse:Username>Customer4</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordText">XXXXXXXXXX</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
    <wsa5:MessageID>urn:uuid:4feb3efb-a8b4-4227-b253-8542fde3ae2e</wsa5:MessageID>
    <wsa5:To SOAP-ENV:mustUnderstand="1">https://localhost:8443/dss-sts-
api/DssSTSService</wsa5:To>
    <wsa5:Action SOAP-ENV:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa5:Action>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <wst:RequestSecurityToken>
      <wsp:AppliesTo>
        <wsa5:EndpointReference>
          <wsa5:Address>https://localhost:8443/dss-customer-
api/DSSCustomerWebService</wsa5:Address>
```

```

</wsa5:EndpointReference>
</wsp:AppliesTo>
<wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issuer</wst:KeyType>
<wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
<wst:TokenType>http://sts.dss.signalcom.ru/DSSToken</wst:TokenType>
<wst14:InteractiveChallengeResponse>
  <wst14:TextChallengeResponse RefId="http://docs.oasis-open.org/ws-sx/ws-
trust/200802/challenge/PIN">XXXXXXXX</wst14:TextChallengeResponse>
</wst14:InteractiveChallengeResponse>
</wst:RequestSecurityToken>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Таблица 145 Описание полей сообщения RequestSecurityToken

Поле	Тип	Описание
MessageID	String	Уникальный идентификатор сообщения.
To	String	URL-адрес STS.
Action	String	http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue
Address	String	URL-адрес веб-сервиса Cloud DSS.
KeyType	String	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issuer
RequestType	String	http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue
TokenType	String	http://sts.dss.signalcom.ru/DSSToken
InteractiveChallengeResponse	InteractiveChallengeResponseType	В данном сообщении используется для отправки PIN-кода (см. Таблица 151).

В случае успешной аутентификации STS посылает пользователю сообщение-ответ RequestSecurityTokenResponseCollection (RSTRC) следующего вида:

```

<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wss="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <S:Header>
    <Action xmlns="http://www.w3.org/2005/08/addressing"
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" S:mustUnderstand="1">http://docs.oasis-
open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal</Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">uuid:c512d97c-b064-4181-
be47-818bac1542a2</MessageID>
    <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:4feb3efb-a8b4-
4227-b253-8542fde3ae2e</RelatesTo>
    <To
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymous<
/To>
    <wsse:Security S:mustUnderstand="1">
      <wsu:Timestamp xmlns:ns14="http://docs.oasis-open.org/ws-sx/ws-
secureconversation/200512" xmlns:ns13="http://www.w3.org/2003/05/soap-envelope" wsu:Id="_1">
        <wsu:Created>2021-03-18T12:50:25Z</wsu:Created>

```

```

        <wsu:Expires>2021-03-18T12:55:25Z</wsu:Expires>
    </wsu:Timestamp>
</wsse:Security>
</S:Header>
<S:Body>
    <trust:RequestSecurityTokenResponseCollection
xmlns:ns10="http://www.w3.org/2000/09/xmldsig#" xmlns:ns13="http://www.w3.org/2001/10/xml-
exc-c14n#" xmlns:ns6="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
xmlns:ns7="http://docs.oasis-open.org/ws-sx/ws-trust/200512/"
xmlns:ns9="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity" xmlns:sc="http://docs.oasis-
open.org/ws-sx/ws-secureconversation/200512" xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
        <trust:RequestSecurityTokenResponse>
            <trust:TokenType>http://sts.dss.signalcom.ru/DSSToken</trust:TokenType>
            <trust:RequestedSecurityToken>
                <DSSToken:DSSToken xmlns="http://sts.dss.signalcom.ru/"
xmlns:DSSToken="http://sts.dss.signalcom.ru/">
                    <AccessToken>04afd122-d48d-4478-ba7d-3f2dce4ac045</AccessToken>
                </DSSToken:DSSToken>
            </trust:RequestedSecurityToken>
            <wsp:AppliesTo>
                <wsa:EndpointReference>
                    <wsa:Address>https://localhost:8443/dss-customer-
api/DSSCustomerWebService</wsa:Address>
                </wsa:EndpointReference>
            </wsp:AppliesTo>
            <trust:Lifetime>
                <wsu:Created>2021-03-18T12:50:25.157Z</wsu:Created>
                <wsu:Expires>2021-03-18T12:51:01.157Z</wsu:Expires>
            </trust:Lifetime>
        </trust:RequestSecurityTokenResponse>
    </trust:RequestSecurityTokenResponseCollection>
</S:Body>
</S:Envelope>

```

XML-схема элемента DSSToken, содержащего маркер доступа Cloud DSS, приведена ниже:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" targetNamespace="http://sts.dss.signalcom.ru/"
xmlns:tns="http://sts.dss.signalcom.ru/" xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault='qualified'>
    <xs:import namespace="http://www.w3.org/XML/1998/namespace"
schemaLocation="http://www.w3.org/2001/xml.xsd"/>
    <xs:element name="DSSToken" type="tns:DSSTokenType"/>
    <xs:complexType name="DSSTokenType">
        <xs:sequence>
            <xs:element name="AccessToken" type="xs:string"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>

```

Если для получения маркера доступа требуется вторичная аутентификация, STS посылает сообщение-ответ RequestSecurityTokenResponse (RSTR) следующего вида:

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <S:Header>
    <Action xmlns="http://www.w3.org/2005/08/addressing"
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" S:mustUnderstand="1">http://docs.oasis-
open.org/ws-sx/ws-trust/200512/RSTRC/IssueFinal</Action>
    <MessageID xmlns="http://www.w3.org/2005/08/addressing">uuid:b79dc937-f408-4c71-
b691-2ce752071ad0</MessageID>
    <RelatesTo xmlns="http://www.w3.org/2005/08/addressing">urn:uuid:0fcd4430-f0d1-
406d-a734-0ee231524050</RelatesTo>
    <To
xmlns="http://www.w3.org/2005/08/addressing">http://www.w3.org/2005/08/addressing/anonymous<
/To>
    <wsse:Security S:mustUnderstand="1">
      <wsu:Timestamp xmlns:ns14="http://docs.oasis-open.org/ws-sx/ws-
secureconversation/200512" xmlns:ns13="http://www.w3.org/2003/05/soap-envelope" wsu:Id="_1">
        <wsu:Created>2021-03-18T06:55:14Z</wsu:Created>
        <wsu:Expires>2021-03-18T07:00:14Z</wsu:Expires>
      </wsu:Timestamp>
    </wsse:Security>
  </S:Header>
  <S:Body>
    <trust:RequestSecurityTokenResponse
xmlns:ns10="http://www.w3.org/2000/09/xmldsig#" xmlns:ns13="http://docs.oasis-open.org/ws-
sx/ws-trust/200802" xmlns:ns14="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ns6="http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd"
xmlns:ns7="http://docs.oasis-open.org/ws-sx/ws-trust/200512/"
xmlns:ns9="http://schemas.xmlsoap.org/ws/2006/02/addressingidentity" xmlns:sc="http://docs.oasis-
open.org/ws-sx/ws-secureconversation/200512" xmlns:trust="http://docs.oasis-open.org/ws-sx/ws-
trust/200512" xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wst="http://schemas.xmlsoap.org/ws/2005/02/trust" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <ns13:InteractiveChallenge>
        <ns13:Title>Test Title</ns13:Title>
        <ns13:TextChallenge Label="Test Label" RefID="http://docs.oasis-open.org/ws-
sx/ws-trust/200802/challenge/OTP"/>
        <ns13:ContextData RefID="94604104"/>
      </ns13:InteractiveChallenge>
    </trust:RequestSecurityTokenResponse>
  </S:Body>
</S:Envelope>
```

Таблица 146 Описание полей структуры InteractiveChallenge

Поле	Тип	Описание
Title	String	Текст заголовка, отображаемый для пользователя (например, заголовок, описывающий цель или характер задачи).
TextChallenge	TextChallengeType	Параметры задачи, требующей текстового ввода от пользователя (см. Таблица 147).
ContextData	ContextDataType	Используется для отправки идентификатора транзакции (см. Таблица 148).



Таблица 147 Описание полей структуры TextChallengeType

Поле	Тип	Описание
RefID	String	Тип параметра аутентификации, запрашиваемого у пользователя (см. Таблица 149).
Label	String	Текст метки для элемента текстового запроса (например, метку для поля ввода текста), которая будет показана пользователю.

Таблица 148 Описание полей структуры ContextDataType

Поле	Тип	Описание
RefID	String	Идентификатор транзакции. Используется для получения маркера доступа и для подтверждения операции пользователя. Если для получения маркера доступа требуется вторичная аутентификация, идентификатор транзакции формируется на стороне STS и отправляется пользователю в сообщении RSTR. При подтверждении операции идентификатор транзакции формируется на стороне веб-сервиса Cloud DSS (см. п. 3.2) и отправляется пользователем в сообщении RST.

Таблица 149 Идентификаторы параметров аутентификации

Идентификатор	Описание
<a href="http://docs.oasis-open.org/ws-sx/ws-trust/200802/challenge/PIN">http://docs.oasis-open.org/ws-sx/ws-trust/200802/challenge/PIN</a>	PIN-код.
<a href="http://docs.oasis-open.org/ws-sx/ws-trust/200802/challenge/OTP">http://docs.oasis-open.org/ws-sx/ws-trust/200802/challenge/OTP</a>	ОТР.

Поле ContextData содержит идентификатор транзакции, сформированный на стороне STS (см. Таблица 148). Этот же идентификатор должен задаваться в следующем сообщении пользователя.

После ввода ОТР пользователь посылает STS сообщение-ответ RequestSecurityTokenResponse (RSTR) следующего вида (см. Таблица 150):

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:c14n="http://www.w3.org/2001/10/xml-
exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml1="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xenc="http://www.w3.org/2001/04/xmenc#" xmlns:wsc="http://docs.oasis-open.org/ws-
secureconversation/200512" xmlns:sts="http://sts.dss.signalcom.ru/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:chan="http://schemas.microsoft.com/ws/2005/02/duplex"
xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:auth="http://docs.oasis-
open.org/wsfed/authorization/200706" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-
open.org/ws-sx/ws-trust/200802">
  <SOAP-ENV:Header>
    <wsse:Security SOAP-ENV:mustUnderstand="1">
      <wsse:UsernameToken wsu:Id="User">
```

```
<wsse:Username>Customer4</wsse:Username>
<wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordText">XXXXXXXXXX</wsse:Password>
</wsse:UsernameToken>
</wsse:Security>
<wsa5:MessageID>urn:uuid:631227f4-e413-4df0-afee-de56ff4e9d90</wsa5:MessageID>
<wsa5:To SOAP-ENV:mustUnderstand="1">https://localhost:8443/dss-sts-
api/DssSTSService</wsa5:To>
<wsa5:Action SOAP-ENV:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RSTR/Issue</wsa5:Action>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<wst:RequestSecurityTokenResponse>
<wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
<wst14:InteractiveChallengeResponse>
<wst14:TextChallengeResponse RefId="http://docs.oasis-open.org/ws-sx/ws-
trust/200802/challenge/OTP">868662</wst14:TextChallengeResponse>
<wst14:ContextData RefId="94604104"></wst14:ContextData>
</wst14:InteractiveChallengeResponse>
</wst:RequestSecurityTokenResponse>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Таблица 150 Описание полей сообщения RequestSecurityTokenResponse пользователя

Поле	Тип	Описание
Action	String	<a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue">http://docs.oasis-open.org/ws-sx/ws-trust/200512/RSTR/Issue</a>
RequestType	String	<a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue">http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue</a>
InteractiveChallengeResponse	InteractiveChallengeResponseType	Используется для отправки OTP (см. Таблица 151).

Таблица 151 Описание полей структуры InteractiveChallengeResponse

Поле	Тип	Описание
TextChallengeResponse	TextChallengeResponseType	Используется для отправки параметров аутентификации пользователя (см. Таблица 152).
ContextData	ContextDataType	Используется для отправки идентификатора транзакции (см. Таблица 148).

Таблица 152 Описание полей структуры TextChallengeResponseType

Поле	Тип	Описание
RefID	String	Тип параметра аутентификации (см. Таблица 149).

В поле ContextData задается идентификатор транзакции, сформированный на стороне STS (см. Таблица 148).

В случае успешной вторичной аутентификации STS посылает пользователю сообщение-ответ RequestSecurityTokenResponseCollection (RSTRC), содержащее маркер доступа (см. выше).

## 6.2.2. Подтверждение операции пользователя

Для подтверждения операции (см. п. 3.2) пользователь посылает STS сообщение-запрос RequestSecurityToken (RST) следующего вида (см. Таблица 145):

```

<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:c14n="http://www.w3.org/2001/10/xml-
exc-c14n#" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:saml1="urn:oasis:names:tc:SAML:1.0:assertion"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:xenc="http://www.w3.org/2001/04/xmenc#" xmlns:wsc="http://docs.oasis-open.org/ws-sx/ws-
secureconversation/200512" xmlns:sts="http://sts.dss.signalcom.ru/" xmlns:wsse="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:chan="http://schemas.microsoft.com/ws/2005/02/duplex"
xmlns:wsa5="http://www.w3.org/2005/08/addressing" xmlns:auth="http://docs.oasis-
open.org/wsfed/authorization/200706" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512" xmlns:wst14="http://docs.oasis-
open.org/ws-sx/ws-trust/200802">
  <SOAP-ENV:Header>
    <wsse:Security SOAP-ENV:mustUnderstand="1">
      <wsse:UsernameToken wsu:Id="User">
        <wsse:Username>Customer4</wsse:Username>
        <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
username-token-profile-1.0#PasswordText">XXXXXXXXXX</wsse:Password>
      </wsse:UsernameToken>
    </wsse:Security>
    <wsa5:MessageID>urn:uuid:0f369bd9-b131-44df-9a1a-
d885d84d81ca</wsa5:MessageID>
    <wsa5:To SOAP-ENV:mustUnderstand="1">https://localhost:8443/dss-sts-
api/DssSTSService</wsa5:To>
    <wsa5:Action SOAP-ENV:mustUnderstand="1">http://docs.oasis-open.org/ws-sx/ws-
trust/200512/RST/Issue</wsa5:Action>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <wst:RequestSecurityToken>
      <wsp:AppliesTo>
        <wsa5:EndpointReference>
          <wsa5:Address>https://localhost:8443/dss-customer-
api/DSSCustomerWebService</wsa5:Address>
        </wsa5:EndpointReference>
      </wsp:AppliesTo>
      <wst:KeyType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Bearer</wst:KeyType>
      <wst:RequestType>http://docs.oasis-open.org/ws-sx/ws-
trust/200512/Issue</wst:RequestType>
      <wst:TokenType>http://sts.dss.signalcom.ru/DSSToken</wst:TokenType>
      <wst14:InteractiveChallengeResponse>
        <wst14:TextChallengeResponse RefId="http://docs.oasis-open.org/ws-sx/ws-
trust/200802/challenge/PIN">XXXXXXXXXX</wst14:TextChallengeResponse>
        <wst14:ContextData RefID="94604105"></wst14:ContextData>
      </wst14:InteractiveChallengeResponse>
    </wst:RequestSecurityToken>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

Данное сообщение аналогично сообщению-запросу RequestSecurityToken (RST), посылаемому пользователем для получения маркера доступа, за исключением дополнительного параметра ContextData, в котором задается идентификатор транзакции, полученный от веб-сервиса Cloud DSS (см. п. 3.2).

---

Остальные сообщения, которыми обмениваются STS и пользователь для подтверждения операции, аналогичны сообщениям, описанным в п. 6.2.1 для случая вторичной аутентификации.

Использование полученного от STS при подтверждении операции маркера доступа является опциональным: для продолжения выполнения операции можно использовать выданный ранее действительный маркер доступа.

## ПРИЛОЖЕНИЕ А. ВЗАИМОДЕЙСТВИЕ КЛИЕНТА С ВЕБ-СЕРВИСОМ ИДЕНТИФИКАЦИИ ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

soapaction: "http://impl.api.identity.dss.signalcom.ru/DSSIdentityWebService/getTokenRequest"  
user-agent: Metro/2.3.1 (UNKNOWN\_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-  
RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-  
revision#unknown

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenRequest
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="bc2b0a6e-05f7-4716-85e1-
ce168e5af0e0"><ns2:authentication><ns2:issuer></ns2:issuer><ns2:subject
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:DssIdentityServiceSubjectInternal"><ns2:value>new_tp@tp.ru</ns2:value><ns2:passw
ord>111111</ns2:password></ns2:subject><ns2:expired>0</ns2:expired><ns2:responseType>code</
ns2:responseType><ns2:clientId>dss-identity-test1-
cust</ns2:clientId><ns2:redirectUri>http://localhost:8080/dss-customer-
web/callback?client_name=GenericOAuth20Client</ns2:redirectUri><ns2:scope>read%20write%20fo
o%20bar</ns2:scope><ns2:state>34refdgfbrty6576yth</ns2:state><ns2:operationId>:0D26B746E962
EC8D7AB67B32D608AD55</ns2:operationId></ns2:authentication></ns3:GetTokenRequest></S:Bo
dy></S:Envelope>-----
```

---[HTTP response 200]---

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenResponse
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="bc2b0a6e-05f7-4716-85e1-
ce168e5af0e0"><ns2:Result><ns2:ResultMajor>ResponderError</ns2:ResultMajor><ns2:ResultMinor
>ErrorFailedSecondFactor</ns2:ResultMinor><ns2:ResultMessage xml:lang="UTF-
8">JUVNQIIMJdCi0YDQsNC90LfQsNC60YbQuNGPIDk0NjA0MDA3LiDQktGF0L7QtCDQsiDQ
v9GA0LjQu9C+0LbQtdC90LjQtS4gINCS0LLQtC00LjRgtC1INC60L7QtCDQuNC3INC/0L7Rh9G
C0L7QtStC+0LPQviDRgdC+0L7QsdGJ0LXQvdC40Y8u</ns2:ResultMessage></ns2:Result></ns3:Ge
tTokenResponse></S:Body></S:Envelope>-----
```

<ns2:ResultMessage xml:lang="UTF-8">=%EMAIL%Транзакция 94604007. Вход в приложение.  
Введите код из почтового сообщения."

---[HTTP request]---

```
accept: text/xml, multipart/related
cache-control: no-cache
connection: keep-alive
content-length: 1034
content-type: text/xml; charset=utf-8
host: 192.168.0.13:8080
pragma: no-cache
soapaction: "http://impl.api.identity.dss.signalcom.ru/DSSIdentityWebService/getTokenRequest"
user-agent: Metro/2.3.1 (UNKNOWN_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-
RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-
revision#unknown
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenRequest
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="55eb3f60-249d-4088-ba28-
104a2155f5e3"><ns2:authentication><ns2:issuer></ns2:issuer><ns2:subject
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:DssIdentityServiceSubjectInternal"><ns2:value>new_tp@tp.ru</ns2:value><ns2:passw
ord>111111</ns2:password></ns2:subject><ns2:expired>0</ns2:expired><ns2:responseType>code</
ns2:responseType><ns2:clientId>dss-identity-test1-
cust</ns2:clientId><ns2:redirectUri>http://localhost:8080/dss-customer-
```

---

```
web/callback?client_name=GenericOAuth20Client</ns2:redirectUri><ns2:scope>read+write+foo+bar
</ns2:scope><ns2:state>34refdgfbrtyt6576yth</ns2:state><ns2:operationId>:0D26B746E962EC8D7A
B67B32D608AD55</ns2:operationId><ns2:confirmationCode>210982</ns2:confirmationCode></ns2
:authentication></ns3:GetTokenRequest></S:Body></S:Envelope>-----
```

---[HTTP response 200]---

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenResponse
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="55eb3f60-249d-4088-ba28-
104a2155f5e3"><ns2:Result><ns2:ResultMajor>ResponderError</ns2:ResultMajor><ns2:ResultMino
r>ErrorFailedPincode</ns2:ResultMinor></ns2:Result></ns3:GetTokenResponse></S:Body></S:Enve
lope>-----
```

---[HTTP request]---

```
accept: text/xml, multipart/related
cache-control: no-cache
connection: keep-alive
content-length: 1059
content-type: text/xml; charset=utf-8
host: 192.168.0.13:8080
pragma: no-cache
soapaction: "http://impl.api.identity.dss.signalcom.ru/DSSIdentityWebService/getTokenRequest"
user-agent: Metro/2.3.1 (UNKNOWN_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-
RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-
revision#unknown
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenRequest
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="5fb629b7-e5aa-4af2-86da-
3b7b5ed13c20"><ns2:authentication><ns2:issuer></ns2:issuer><ns2:subject
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:DssIdentityServiceSubjectInternal"><ns2:value>new_tp@tp.ru</ns2:value><ns2:passw
ord>111111</ns2:password></ns2:subject><ns2:expired>0</ns2:expired><ns2:pin>111111</ns2:pin>
<ns2:responseType>code</ns2:responseType><ns2:clientId>dss-identity-test1-
cust</ns2:clientId><ns2:redirectUri>http://localhost:8080/dss-customer-
web/callback?client_name=GenericOAuth20Client</ns2:redirectUri><ns2:scope>read+write+foo+bar
</ns2:scope><ns2:state>34refdgfbrtyt6576yth</ns2:state><ns2:operationId>:0D26B746E962EC8D7A
B67B32D608AD55</ns2:operationId><ns2:confirmationCode>210982</ns2:confirmationCode></ns2
:authentication></ns3:GetTokenRequest></S:Body></S:Envelope>-----
```

---[HTTP response 200]---

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenResponse
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="5fb629b7-e5aa-4af2-86da-
3b7b5ed13c20"><ns2:Result><ns2:ResultMajor>Success</ns2:ResultMajor></ns2:Result><ns2:token
>9dde77b1-fa16-4999-bb1e-
cce1dcf4c42f</ns2:token></ns3:GetTokenResponse></S:Body></S:Envelope>-----
```

## ПРИЛОЖЕНИЕ Б. ВЗАИМОДЕЙСТВИЕ КЛИЕНТА С ВЕБ-СЕРВИСОМ ПОЛЬЗОВАТЕЛЯ И ВЕБ-СЕРВИСОМ ИДЕНТИФИКАЦИИ ПРИ ПОДТВЕРЖДЕНИИ ОПЕРАЦИИ ПОЛЬЗОВАТЕЛЯ

---[HTTP request]---

```
accept: text/xml, multipart/related
cache-control: no-cache
connection: keep-alive
content-length: 1762
content-type: text/xml; charset=utf-8
host: dss-ws.signal-com.ru:8080
pragma: no-cache
soapaction: "http://server.customer.dss.signalcom.ru/DSSCustomerWebService/signRequest"
user-agent: Metro/2.3.1 (UNKNOWN_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-
RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-
revision#unknown
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns9:SignRequest
xmlns:ns3="http://verificationreport.dss.signalcom.ru/"
xmlns:ns4="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns5="http://commontypes.dss.signalcom.ru/"
xmlns:ns6="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns7="http://www.w3.org/2001/04/xmenc#" xmlns:ns8="http://api.customer.dss.signalcom.ru/"
xmlns:ns9="http://server.customer.dss.signalcom.ru/" RequestID="98bae9a9-1cac-4d0b-b313-
958507722773"><ns8:OptionalInputs><AccessToken>192ec13d-2fb6-48ae-906f-
9d7cf12b31af</AccessToken></ns8:OptionalInputs><InputDocument Name="РЎРµСЃС, PsPIC<P№
PrPsPeCfPjPµPSC, "><ns5:Document><ns5:Base64Data>///4NAAoAWwAuAFMAaABlAGwAbABD
AGwAYQBzAHMASQBuAGYAbwBdAA0ACgBMAG8AYwBhAGwAaQB6AGUAZABSAGUAc
wBvAHUAcgBjAGUATgBhAG0AZQA9AEAAJQBTAHkAcwB0AGUAbQBSAG8AbwB0ACUAX
ABzAHkAcwB0AGUAbQAzADIAxABzAGgAZQBzAGwAMwAyAC4AZABsAGwALAAAtADIAM
QA3ADkAOQANAAoAWwBMAG8AYwBhAGwAaQB6AGUAZABGAGkAbABIAE4AYQBtAGU
AcwBdAA0ACgBXAGkAbABkAFQAYQBuAGcAZQBwAHQAIAHBHAGEAbQBIAHMAIABBAH
AAcAAgAC0AIABhAHMAdQBzAC4AbABuAGsAPQBAAEMAOGbCFAAAUgBPAAEcAUgBBAH
4AMgBcAFcASQBMAEQAVABBAH4AMQBcAFQATwBVAEMASABQAH4AMQBcAGEAcwB1
AHMAXABNAFUASQBMAgkAbgBrAC4AZQB4AGUALAAAtADEAMAA1AA0ACgBDAHkAYg
BIAHIATABpAG4AawAgAE0AZQBkAGkAYQBTAHQAbwByAHkALgBsAG4AawA9AEAAQwA
6AFwAUABSAE8ARwBSAEAAfgAyAFwAQQBTAfUAUwBcAE0ARQBEAEkAQQBTAH4AMQ
BcAE0AVQBJAFQAUgBBAH4AMQBcAE0ARABTAE0AVQBJAH4AMQAuAEQATABMACwA
LQAxADAANAANAoA</ns5:Base64Data></ns5:Document></InputDocument><SignatureType>C
MS</SignatureType><SignParameters><ns5:CMSSignParameters><Detached>true</Detached></ns5:
CMSSignParameters></SignParameters><KeySelector><KeyName>6c41aa13-e6fc-415c-9ed6-
4886e6302f76</KeyName></KeySelector></ns9:SignRequest></S:Body></S:Envelope>-----
-----
```

---[HTTP response 200]---

```
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns9:SignResponse
xmlns:ns3="http://api.customer.dss.signalcom.ru/" xmlns:ns4="http://commontypes.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns6="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns7="http://www.w3.org/2001/04/xmenc#"
xmlns:ns8="http://verificationreport.dss.signalcom.ru/"
xmlns:ns9="http://server.customer.dss.signalcom.ru/" RequestID="98bae9a9-1cac-4d0b-b313-
958507722773"><ns3:Result><ns3:ResultMajor>Success</ns3:ResultMajor><ns3:ResultMinor>Confi
rmationRequired</ns3:ResultMinor></ns3:Result><ns3:OptionalOutputs><TransactionID>94604009<
/TransactionID></ns3:OptionalOutputs></ns9:SignResponse></S:Body></S:Envelope>-----
--
```

---[HTTP request]---

---

```

accept: text/xml, multipart/related
cache-control: no-cache
connection: keep-alive
content-length: 1252
content-type: text/xml; charset=utf-8
host: 192.168.0.13:8080
pragma: no-cache
soapaction: "http://impl.api.identity.dss.signalcom.ru/DSSIdentityWebService/getTokenRequest"
user-agent: Metro/2.3.1 (UNKNOWN_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-
RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-
revision#unknown
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenRequest
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="d45de6e4-870d-4c25-8c40-
7d745b8b1acf"><ns2:authentication><ns2:issuer></ns2:issuer><ns2:subject
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ns2:DssIdentityServiceSubjectInternal"><ns2:value>new_tp@tp.ru</ns2:value><ns2:passw
ord>111111</ns2:password></ns2:subject><ns2:expired>0</ns2:expired><ns2:pin>111111</ns2:pin>
<ns2:responseType>code</ns2:responseType><ns2:clientId>dss-identity-test1-cust-
confirm</ns2:clientId><ns2:redirectUri>http://localhost:8080/dss-customer-
web/oauth2client/authorization_code</ns2:redirectUri><ns2:scope>%D0%9F%D0%BE%D0%B4%D
1%82%D0%B2%D0%B5%D1%80%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5+%D0
%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8+%D0%BF%D0%BE%D0
%B4%D0%BF%D0%B8%D1%81%D0%B8+%D1%84%D0%B0%D0%B9%D0%BB%D0%B0.</ns2
:scope><ns2:state>0d1dbf10-4256-45a9-97c2-
9945f3a5be45</ns2:state><ns2:operationId>94604009</ns2:operationId><ns2:accessToken>192ec13d
-2fb6-48ae-906f-
9d7cf12b31af</ns2:accessToken></ns2:authentication></ns3:GetTokenRequest></S:Body></S:Envel
ope>-----

```

<ns2:scope>="Подтверждение операции подписи файла."

```

05-Feb-2021 23:41:02.490 INFO [http-nio-8080-exec-11]
ru.signalcom.dss.webserver.wicket.pages.CustomerPageSignDocument$1$1.confirmTransaction
Creating new operation for signing file
---[HTTP response 200]---
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenResponse
xmlns:ns2="http://api.identity.dss.signalcom.ru/"
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="d45de6e4-870d-4c25-8c40-
7d745b8b1acf"><ns2:Result><ns2:ResultMajor>ResponderError</ns2:ResultMajor><ns2:ResultMino
r>ErrorFailedSecondFactor</ns2:ResultMinor><ns2:ResultMessage xml:lang="UTF-
8">JUVNQIIMJdCi0YDQsNC90LfQsNC60YbQuNGPIDk0NjA0MDA5LiDQn9C+0LTQv9C40YH
QsNC90LjQtSDQtNC+0LrRg9C80LXQvdGC0LAuINCi0LXRgdGC0L7QstGL0Lkg0LTQvtC60YPQ
vNC10L3RgiDQktCy0LXQtNC40YLQtSDQtC+0LQg0LjQtyDQv9C+0YfRgtC+0LLQvtCz0L4g0Y
HQvtC+0LHRidC10L3QuNGPLg==</ns2:ResultMessage></ns2:Result></ns3:GetTokenResponse></
S:Body></S:Envelope>-----

```

<ns2:ResultMessage xml:lang="UTF-8">="EMAIL%Транзакция 94604009. Подписание документа. Тестовый документ Введите код из почтового сообщения."

```

---[HTTP request]---
accept: text/xml, multipart/related
cache-control: no-cache
connection: keep-alive
content-length: 1303
content-type: text/xml; charset=utf-8
host: 192.168.0.13:8080

```



---

pragma: no-cache  
soapaction: "http://impl.api.identity.dss.signalcom.ru/DSSIdentityWebService/getTokenRequest"  
user-agent: Metro/2.3.1 (UNKNOWN\_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-revision#unknown  
<?xml version='1.0' encoding='UTF-8'?><S:Envelope  
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenRequest  
xmlns:ns2="http://api.identity.dss.signalcom.ru/"  
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="b8ac2c49-9c73-4614-8a9b-b78a3631e5ca"><ns2:authentication><ns2:issuer></ns2:issuer><ns2:subject  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xsi:type="ns2:DssIdentityServiceSubjectInternal"><ns2:value>new\_tp@tp.ru</ns2:value><ns2:password>111111</ns2:password></ns2:subject><ns2:expired>0</ns2:expired><ns2:pin>111111</ns2:pin>  
<ns2:responseType>code</ns2:responseType><ns2:clientId>dss-identity-test1-cust-confirm</ns2:clientId><ns2:redirectUri>http://localhost:8080/dss-customer-web/oauth2client/authorization\_code</ns2:redirectUri><ns2:scope>%D0%9F%D0%BE%D0%B4%D1%82%D0%B2%D0%B5%D1%80%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5+%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%B8+%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D0%B8+%D1%84%D0%B0%D0%B9%D0%BB%D0%B0.</ns2:scope><ns2:state>0d1dbf10-4256-45a9-97c2-9945f3a5be45</ns2:state><ns2:operationId>94604009</ns2:operationId><ns2:confirmationCode>842823</ns2:confirmationCode><ns2:accessToken>192ec13d-2fb6-48ae-906f-9d7cf12b31af</ns2:accessToken></ns2:authentication></ns3:GetTokenRequest></S:Body></S:Envelope>-----

<ns2:scope>="Подтверждение операции подписи файла."

---[HTTP response 200]---

<?xml version='1.0' encoding='UTF-8'?><S:Envelope  
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns3:GetTokenResponse  
xmlns:ns2="http://api.identity.dss.signalcom.ru/"  
xmlns:ns3="http://impl.api.identity.dss.signalcom.ru/" RequestID="b8ac2c49-9c73-4614-8a9b-b78a3631e5ca"><ns2:Result><ns2:ResultMajor>Success</ns2:ResultMajor></ns2:Result><ns2:token>2f0caf0a-a542-4250-9a00-3fb4c8ff2022</ns2:token></ns3:GetTokenResponse></S:Body></S:Envelope>-----

---[HTTP request]---

accept: text/xml, multipart/related

cache-control: no-cache

connection: keep-alive

content-length: 710

content-type: text/xml; charset=utf-8

host: dss-ws.signal-com.ru:8080

pragma: no-cache

soapaction: "http://server.customer.dss.signalcom.ru/DSSCustomerWebService/signRequest"

user-agent: Metro/2.3.1 (UNKNOWN\_BRANCH-false; 2015-01-15T16:53:43+0100) JAXWS-RI/2.2.10 JAXWS-API/2.2.11 JAXB-RI/2.2.10-b140802.1033 JAXB-API/2.2.12-b140109.1041 svn-revision#unknown

<?xml version='1.0' encoding='UTF-8'?><S:Envelope  
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns9:SignRequest  
xmlns:ns3="http://verificationreport.dss.signalcom.ru/"  
xmlns:ns4="http://www.w3.org/2000/09/xmldsig#"  
xmlns:ns5="http://commontypes.dss.signalcom.ru/"  
xmlns:ns6="urn:oasis:names:tc:SAML:2.0:assertion"  
xmlns:ns7="http://www.w3.org/2001/04/xmenc#" xmlns:ns8="http://api.customer.dss.signalcom.ru/"  
xmlns:ns9="http://server.customer.dss.signalcom.ru/" RequestID="56ca70cf-524d-44b7-8000-cc738623a1bd"><ns8:OptionalInputs><AccessToken>2f0caf0a-a542-4250-9a00-3fb4c8ff2022</AccessToken><TransactionID>94604009</TransactionID></ns8:OptionalInputs></ns9:SignRequest></S:Body></S:Envelope>-----

```
05-Feb-2021 23:41:28.846 INFO [http-nio-8080-exec-2]
[com.sun.xml.ws.policy.parser.PolicyConfigParser].parse WSP5018: Loaded WSIT configuration
from file: jar:file:/H:/tmp/tomcat_sts/shared/lib/hsm-client.jar!/META-INF/wsit-client.xml.
---[HTTP response 200]---
<?xml version='1.0' encoding='UTF-8'?><S:Envelope
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"><S:Body><ns9:SignResponse
xmlns:ns3="http://api.customer.dss.signalcom.ru/" xmlns:ns4="http://commontypes.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns6="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns7="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns8="http://verificationreport.dss.signalcom.ru/"
xmlns:ns9="http://server.customer.dss.signalcom.ru/" RequestID="56ca70cf-524d-44b7-8000-
cc738623a1bd"><ns3:Result><ns3:ResultMajor>Success</ns3:ResultMajor><ns3:ResultMinor>Opera
tionCompleted</ns3:ResultMinor></ns3:Result><SignatureObject><ns4:Base64Signature
Type="CMS">MIAGCSqGSIB3DQEHAQcAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSq
GSIB3DQEHAQAaOIIETCCBCEwggPmoAMCAQICCG7Aaj86ATcCCTowDAYIKoUDbwEBaw
IFADBNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5Ta
WduYWtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMTItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQHRwLnJlMRswGQYJKoZIhvcNAQkBF
gxuZXdfdHBAdHAucnUwZjAfBggqhQMHAQEBATATBgcqhQMCAiQABggqhQMHAQECAgND
AARACBxSdlb5PCh4njiIyck4ynwV2ESXuTrIM2K1vUNoT7xTpIHE5I/BBO+7JFZNgnEY1XL2Qw
BmkRs1n1cl4iAlfqOCAM4wggJqMAwGA1UdEWB/wQCMAAwHQYDVR0OBByEFASothhH9C
+O0riHS9gfEFoaBU+2MIGYBgNVHSMegZAwgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaT
BNMQswCQYDVQQGEwJSVTEPMAMGA1UEBwwGTW9zYyZy293MRcwFQYDVQQKDA5TaWduY
WwtMjU09NIEpTQzEuMCwGA1UEAwZlZS1Ob3RhenkgVGZzdCBDQSAOR09TVFIzNDEwLTIwMT
ItMjU0ZTAeFw0yMTAxMjgyMjMzMjVAFw0yMTAxMjgyMjMzMjVAMEGxCzAJBgNVBA
YTAIYVMRwwGgYDVQQDBDQndC+0LLRI9C5IHRRwQ
```

## ПРИЛОЖЕНИЕ В. ПРИМЕРЫ ЗАПРОСОВ

Пример создания пользователя Cloud DSS (см. п. 3.4.4):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AddCustomerRequest RequestID="1f639e36-0758-4794-a4d4-e9d1ea57769c"
xmlns="http://api.operator.dss.signalcom.ru/" xmlns:ns5="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <OptionalInputs>
    <AccessToken>a6ca5edc-8744-4dc0-9844-a2d7e6e77231</AccessToken>
  </OptionalInputs>
  <CustomerInfo>
    <ns2:InternalSubject>
      <ns2:Login>customer1</ns2:Login>
    </ns2:InternalSubject>
    <ns2:DisplayName>customer1</ns2:DisplayName>
    <ns2:PhoneNumber>+7(XXX)XXXXXXX</ns2:PhoneNumber>
    <ns2:Email>customer1@example.com</ns2:Email>
    <ns2:AuthenticationMethod>OTP_VIA_SMS</ns2:AuthenticationMethod>
    <ns2:ConfirmedActions>
      <ns2:Action>LOGIN</ns2:Action>
      <ns2:Action>SIGN</ns2:Action>
    </ns2:ConfirmedActions>
    <ns2:UserLocale Language="ru" Country="RU"/>
    <ns2:Transliteration>true</ns2:Transliteration>
    <ns2:SubjectAttributes>
      <ns2:X509NameAttribute oid="urn:oid:2.5.4.6" value="RU"/>
      <ns2:X509NameAttribute oid="urn:oid:2.5.4.3" value="Иванов Иван Иванович"/>
      <ns2:X509NameAttribute oid="urn:oid:1.2.840.113549.1.9.1"
value="customer1@example.com"/>
      <ns2:X509NameAttribute oid="urn:oid:1.2.643.3.131.1.1"
value="XXXXXXXXXXXXXXXX"/>
      <ns2:X509NameAttribute oid="urn:oid:1.2.643.100.3" value="XXXXXXXXXXXXXXXX"/>
    </ns2:SubjectAttributes>
    <ns2:NotificationTransports>
      <ns2:Transport>SMS</ns2:Transport>
    </ns2:NotificationTransports>
    <ns2:Group>3</ns2:Group>
  </CustomerInfo>
</AddCustomerRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AddCustomerResponse RequestID="1f639e36-0758-4794-a4d4-e9d1ea57769c"
xmlns="http://api.operator.dss.signalcom.ru/" xmlns:ns5="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <Result>
    <ResultMajor>Success</ResultMajor>
    <ResultMinor>OperationCompleted</ResultMinor>
  </Result>
  <CustomerID>1155</CustomerID>
  <Password>XXXXXX</Password>
</AddCustomerResponse>
```

Пример создания ключа ЭП и запроса на создание сертификата ключа проверки ЭП (см. п. 3.3.3):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```

    <GenerateKeyPairRequest RequestID="162856e9-6801-4265-ba50-f91665897cfa"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <OptionalInputs>
        <AccessToken>2121ea3d-47a1-4f21-adf5-cd666e1cd19f</AccessToken>
    </OptionalInputs>
    <CertificationRequestInfo>
        <ns2:CAId>1</ns2:CAId>
        <ns2:TemplateId>10</ns2:TemplateId>
    </CertificationRequestInfo>
    <Label>My test key label</Label>
</GenerateKeyPairRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GenerateKeyPairResponse RequestID="162856e9-6801-4265-ba50-f91665897cfa"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <Result>
        <ResultMajor>Success</ResultMajor>
        <ResultMinor>OperationCompleted</ResultMinor>
    </Result>
    <KeySelector>
        <ns2:KeyName>0bb2df99-de18-4d29-9d11-7f0433472331</ns2:KeyName>
    </KeySelector>
</GenerateKeyPairResponse>
  
```

Пример подписания запроса на создание сертификата ключа проверки ЭП пользователя ключом ЭП оператора (см. п. 3.4.9):

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GenerateCustomerCMCRequest RequestID="00fc4c7a-5b2d-4b0c-8a13-73d21acda119"
xmlns="http://api.operator.dss.signalcom.ru/" xmlns:ns5="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <OptionalInputs>
        <AccessToken>b0c489e2-5296-47ae-b784-de6c1c89fef7</AccessToken>
    </OptionalInputs>
    <CustomerID>1155</CustomerID>
    <KeySelector>
        <ns2:KeyName>0bb2df99-de18-4d29-9d11-7f0433472331</ns2:KeyName>
    </KeySelector>
    <SignatureKey>
        <ns2:KeyName>66f9b678-ed1b-411d-b401-30153fada17d</ns2:KeyName>
    </SignatureKey>
    <AddSignerCertificate>true</AddSignerCertificate>
</GenerateCustomerCMCRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GenerateCustomerCMCResponse RequestID="00fc4c7a-5b2d-4b0c-8a13-73d21acda119"
xmlns="http://api.operator.dss.signalcom.ru/" xmlns:ns5="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <Result>
        <ResultMajor>Success</ResultMajor>
        <ResultMinor>OperationCompleted</ResultMinor>
    </Result>
  
```

</Result>  
</GenerateCustomerCMCResponse>

Пример получения информации о ключах ЭП, запросах на создание сертификатов ключей проверки ЭП, сертификатах ключей проверки ЭП и запросах на аннулирование сертификатов ключей проверки ЭП (см. п. 3.3.5):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <GetKeyEntryInfoRequest RequestID="6f79071d-47de-4574-9434-de57ef20d43f"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <OptionalInputs>
        <AccessToken>add0df9a-d892-4248-bef4-3ee393c0bdc1</AccessToken>
    </OptionalInputs>
    <ResultFormat>ASN.1</ResultFormat>
  </GetKeyEntryInfoRequest>

  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
    <GetKeyEntryInfoResponse RequestID="6f79071d-47de-4574-9434-de57ef20d43f"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
        <Result>
            <ResultMajor>Success</ResultMajor>
            <ResultMinor>OperationCompleted</ResultMinor>
        </Result>
        <KeyEntries TotalNumber="1">
            <ns2:KeyEntry>
                <ns2:KeyName>0bb2df99-de18-4d29-9d11-7f0433472331</ns2:KeyName>
                <ns2:Label>My test key label</ns2:Label>
                <ns2:PrivateKeyStartDate>2022-04-
26T12:54:19.849+03:00</ns2:PrivateKeyStartDate>
                <ns2:PrivateKeyEndDate>2023-04-26T12:54:19.849+03:00</ns2:PrivateKeyEndDate>
                <ns2:CertificationRequest>
                    <ns2:EncodedRequest>MIAGCSqGSIb3DQEHAqCAMIACAQMxDjAMBggqhQMHAQECA
gUAMIAGCCsGAQUFBwwCoIAkgASCAecwgGhJMBcwFQIBAQQYIKwYBBQUHBwUxBgIEeUQ
34TCCACkGggG+AgECMIIBtzCCAWQCAQAwZjEvMC0GA1UEAwmm0JjQstCw0L3QvtCyINCY
0LLQsNC9INCY0LLQsNC90L7QstC40YcxJjAkBgkqhkiG9w0BCQEFWF3kua2ludHNvdKbZaWduY
WwtY29tLnJ1MQswCQYDVQQGEwJSVtBmMB8GCCqFAwcBAQEBMBMGBByqFAwICJAAGC
CqFAwcBAQICA0MABEAO0SF/FWTIWRgssyzjzhliwsqIkmiDIHScx1MNy1QwJ3LLTG38t8Bysr
oX6KOKt1pwEXMJ+xs1bIgOlc6Us5zoIGOMIGLBgkqhkiG9w0BCQ4xfjB8MAwGA1UdEwEB/wQ
CMAAwDgYDVR0PAQH/BAQDAgP4MB0GA1UdJQQWMBQGCCsGAQUFBwMEBgggrBgEFBQ
cDAjATBgNVHSAEDDAKMAGGBiqFA2RxATAoBgUqhQnkbwQfDB3QodCa0JfQmCAiU2lnbmF
sLUNPTSBKQ1AgMy4xIjAKBgqqhQMHAQEDAgNBALap2f6FXZqktpcTwtaPenEqANYC6Jar5jK
9F9JGWtGC+EQaT/KD5/HSvaGhrpGNkqPkhd+Yoet0bSyGUO/mMQgwADAAAAAAAAAAAAoIIER
TCCBEEwggPuoAMCAQICCG7AkIaATCCCu8wCgYIKoUDBwEBAwIwZzELMAkGA1UEBhMC
UIUxDzANBgNVBACMBk1vc2NvdzEXMBUGA1UECgwOU2lnbmFsLUNPTSBKU0MxLjAsBgNV
BAMMJWUtTm90YXJ5IFRlc3QgQ0EgKEdPU1RSMzQxMC0yMDEyLT11NikwHhcNMjExMDAx
MDY0NTE4WheNMjExMDAxMDY0NTE4WjBEMQswCQYDVQQGEwJSVtETMBEGA1UEAww
KT3BlcmF0b3IzGmZEGMB4GCSqGSIb3DQEJARYRb3BlcmF0b3IzQHRlc3QucnUwZjAfbGggqhQM
HAQEBAATBgqqhQMCAiQABggqhQMHAQECAgNDAARaf56MZbr3j3SnP47wNpl8weq0kXzsum
srt8K1uGPxsLpYdrX/N2sCzLqFch4Y8wh4my6Vh1BzpVIZReE38JrPdf6OCAPYwggKSMawGA1U
dEwEB/wQCMAAwHQYDVR0OBBYEFJu+Rzck5c8cT7+oWGaLLaXnyjTVMIGYBgNVHSMEGZ
AwgY2AFC+9s0CEHTLJBj+DJM1A12bnqf+0oWukaTBmMQswCQYDVQQGEwJSVtEPMAGA1
UEBwwGTW9zY293MRcwFQYDVQQKDA5TaWduYWwtQ209NIEPtQzEwMCwGA1UEAwwLZS1
Ob3RhcngkVG9vdCBQDQSAAR09YTVFlZnNDEwLTIwMTItMjU2Y2YiIAbsBAQE3AQEwHQYDVR0
BBYwFAYIKwYBBQUHAWIGCCsGAQUFBwMEMEIGA1UdHwQ7MDkwN6A1oDOGMWh0dH
A6Lv93d3cuZS1ub3RhcncucnUvY3JsX3Rlc3OvY3JsX2cyMDEyLT11Ni5icmwwNwYIKwYBBQU
```

```

HAQEEKzApMCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcHRlc3QuZS1ub3RhenkucnUwKAYFK
oUDZG8EHwwd0KHQmtCX0JggllNpZ25hbC1DT00gSkNQIDMuMSIwEwYDVR0gBAwwCjAIBg
YqhQNkcQEwga8GBSsqFA2RwBIGIMIGiDBPQodCa0JfQmCAiQ0FEQiAyLjEiDBzQn9CQ0Jog0K
PQpiAiTm90YXJ5LVBSTyAyLjgiDDfQl9Cw0LrQu9GO0YfQtdC90LjQtSDihJYgMTQ5Lzcv
LTE4Njgg0L7RgiAxNC4wOC4yMDE5DDTQl9Cw0LrQu9GO0YfQtdC90LjQtSDihJYgMTQ5Lzcv
Ni0MTQg0L7RgiAyNy4wMy4yMDIwMCsGA1UdEQAQkMCKADzIwMjExMDAxMDY0NTE4W0
EPMjAyMjAxMjkwNjQ1MThtaMA4GA1UdDwEB/wQEAwID+DAKBggqhQMHAQEDAgNBAE6
WdjDNKOHLIXt7iV1TGTaRzED+CcrDd0OskExdfP5Vejejm/26zNH7FEtwOcVVLhp7ssBA/vW3fij
b/vHPGDUxggIPMIICCwIBATB1MGcxCAZJBgNVBAYTAIjVMQ8wDQYDVQQHDAZNb3Njb3c
xFzAVBgNVBAoMDINpZ25hbC1DT00gSINDMS4wLAYDVQQDDCVILU5vdGFyeSBUBUZXN0IEN
BICHT1NUUjM0MTAtMjAxMi0yNTYpAgoBuwJCGgE3AgrvMAwGCCqFAwCBAQICBQCgggE
vMBcGCSqSgSIb3DQEJAzEKBggrBgEFBQcMAjAcBgkqhkiG9w0BCQUxDxcNMjIwNDI2MTAyN
DA5WjAvBgkqhkiG9w0BCQQxIgQsS9dDRxAYyjaBy6kt/hypYqu5MeRpRdzqWjXhqnUrR0wgcQ
GCyqSgSIb3DQEJEAIVMYG0MIGxMIGuMIGrMAwGCCqFAwCBAQICBQAEIjYHcQbOOXcSs7
7/XXInQ2YMIshbtjXn8ZGw1hdCtiCMHkwa6RPMGcxCAZJBgNVBAYTAIjVMQ8wDQYDVQQH
DAZNb3Njb3cxFzAVBgNVBAoMDINpZ25hbC1DT00gSINDMS4wLAYDVQQDDCVILU5vdGFye
SBUBUZXN0IENBICHT1NUUjM0MTAtMjAxMi0yNTYpAgoBuwJCGgE3AgrvMAwGCCqFAwCBA
QEBAQAEQK5iBsl8tpvx1jSDHyFIYiBV5JWxChERvGLZXfqktaVAC+X+WQY5c4iGAF/hMj5eq/n
hzmajLX9PZvtU1XLh8g4AAAAA=
```

<ns2:Status>CERTIFIED</ns2:Status>  
 <ns2:Subject>C=RU, emailAddress= customer1@example.com, CN=Иванов Иван  
 Иванович</ns2:Subject>  
 <ns2:CAId>1</ns2:CAId>  
 </ns2:CertificationRequest>  
 <ns2:X509Certificate>  
 <ns2:EncodedCertificate>MIIEYzCCBBBgAwIBAgIKAbsCQzwBNwJWZDAKBggqhQMHA  
 QEDAJBnMQswCQYDVQQGEwJSVTEPMA0GA1UEBwwGTW9zY293MRcwFQYDVQQKDA5T  
 aWduYWwtQ09NIEpTQzEuMCwGA1UEAwWlZS1Ob3RhenkgVG9VzdCBDQSAoR09TVFIlZnDEw  
 LTIwMTItMjU2KTAeFw0yMjA0MjYxMDI0MDZaFw0yMjEwMjMxMDI0MDZaMGYxCzAJBgNV  
 BAYTAIjVMS8wLQYDVQQDDCbQmNCy0LDQvdC+0LIg0JjQstCw0L0g0JjQstCw0L3QvtCy0LjR  
 hZEmMCQGCSqSgSIb3DQEJARYXeS5raW50c292QHNPZ25hbC1jb20ucnUwZjAfBgqhQMHAQE  
 BATATBgqhQMCAiQABggqhQMHAQECAGNDAARACTtEhfxVkyFkYLMss484SIsLKiJjow5R0  
 nMdTDctUMCdy0xt/LfAcrK6F+ijpLdacBFzCfsbNWYIDpXOIL0c6OCAPYwggKSMawGA1UdE  
 wEB/wQMAAwHQYDVROBBYEFMFARyVkw+uMex6VDuiY96G/jxIFMIGYBgNVHSMegZA  
 wgY2AFC+9s0CEHTLBJ+DJM1A12bnqf+0oWukaTBnMQswCQYDVQQGEwJSVTEPMA0GA1UE  
 EBwwGTW9zY293MRcwFQYDVQQKDA5TaWduYWwtQ09NIEpTQzEuMCwGA1UEAwWlZS1Ob  
 3RhenkgVG9VzdCBDQSAoR09TVFIlZnDEwLTIwMTItMjU2KTYIAbsBAQE3AQEwHQYDVROIB  
 BYwFAyIKwYBBQUHAWIGCCsGAQUFBwMEMEIGA1UdHwQ7MDkwN6A1oDOGMWh0dHA6  
 LQ93d3cuZS1ub3RhenkucnUvY3JsX3Rlc3QvY3JsX2cyMDEyLTU1Ni5jcmwwNwYIKwYBBQUHA  
 QEYzZG8EHwwd0KHQmtCX0JggllNpZ25hbC1DT00gSkNQIDMuMSIwEwYDVR0gBAwwCjAIBgYq  
 hQNkcQEwga8GBSsqFA2RwBIGIMIGiDBPQodCa0JfQmCAiQ0FEQiAyLjEiDBzQn9CQ0Jog0KPQ  
 piAiTm90YXJ5LVBSTyAyLjgiDDfQl9Cw0LrQu9GO0YfQtdC90LjQtSDihJYgMTQ5Lzcv  
 LTE4Njgg0L7RgiAxNC4wOC4yMDE5DDTQl9Cw0LrQu9GO0YfQtdC90LjQtSDihJYgMTQ5LzcvNi0  
 xMTQg0L7RgiAyNy4wMy4yMDIwMCsGA1UdEQAQkMCKADzIwMjIwNDI2MTAyNDA2W0EPMj  
 AyMjA4MjQxMDI0MDZaMA4GA1UdDwEB/wQEAwID+DAKBggqhQMHAQEDAgNBAAhUzljf  
 r3rQRD1OQy4T46b/V0rUWwqXEMu9e/M1QjcD4CuymJcSousTd2P38g7OEJuy8jv895b4ohG51+  
 GgI=

<ns2:CertificateStatus>  
 <ns2:Status>ACTIVE</ns2:Status>  
 </ns2:CertificateStatus>  
 <ns2:Subject>emailAddress=customer1@example.com, CN=Иванов Иван  
 Иванович, C=RU</ns2:Subject>  
 <ns2:Issuer>CN=e-Notary Test CA (GOSTR3410-2012-256), O=Signal-COM JSC,  
 L=Moscow, C=RU</ns2:Issuer>  
 <ns2:NotBefore>2022-04-26T13:24:06.000+03:00</ns2:NotBefore>  
 <ns2:NotAfter>2022-10-23T13:24:06.000+03:00</ns2:NotAfter>  
 <ns2:CAId>1</ns2:CAId>  
 </ns2:X509Certificate>  
 <ns2:PublicKey>

```

        <ns2:Algorithm>urn:oid:1.2.643.7.1.1.1.1</ns2:Algorithm>
        <ns2:GostR3410Params>urn:oid:1.2.643.2.2.36.0</ns2:GostR3410Params>
        <ns2:GostR3411Params>urn:oid:1.2.643.7.1.1.2.2</ns2:GostR3411Params>
        <ns2:Value>CTtEhfxVkyFkYLMss484SIslKiJJow5R0nMdTDctUMCddy0xt/LfAcrK6F+ijpL
        dacBFzCfsbNWyiDpXOILocw==</ns2:Value>
        </ns2:PublicKey>
    </ns2:KeyEntry>
</KeyEntries>
</GetKeyEntryInfoResponse>

```

Пример создания ЭП с подтверждением операции (см. п. 3.3.10). В ответе на первый запрос создания ЭП возвращается идентификатор транзакции, который необходимо использовать для подтверждения операции создания ЭП (см. п. 6.1.3):

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignRequest RequestID="0940ac5d-0bd2-4af5-9d78-3c4d56787e8e"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <OptionalInputs>
        <AccessToken>8515c25c-8ee8-4386-93be-7a10ca7a3c29</AccessToken>
    </OptionalInputs>
    <InputDocument Name="document">
        <ns2:Document>
            <ns2:Base64Data>MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkw</ns2:Base64Data>
        </ns2:Document>
    </InputDocument>
    <SignatureType>CMS</SignatureType>
    <SignParameters>
        <ns2:CMSSignParameters>
            <ns2:Detached>true</ns2:Detached>
        </ns2:CMSSignParameters>
    </SignParameters>
    <KeySelector>
        <ns2:KeyName>0bb2df99-de18-4d29-9d11-7f0433472331</ns2:KeyName>
    </KeySelector>
</SignRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignResponse RequestID="0940ac5d-0bd2-4af5-9d78-3c4d56787e8e"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <Result>
        <ResultMajor>Success</ResultMajor>
        <ResultMinor>ConfirmationRequired</ResultMinor>
    </Result>
    <OptionalOutputs>
        <TransactionID>99549417</TransactionID>
    </OptionalOutputs>
</SignResponse>

```

После подтверждения операции создания ЭП посылается второй запрос на создание ЭП с ограниченным набором параметров (маркер доступа и идентификатор транзакции), в ответе на запрос возвращается ЭП:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignRequest RequestID="ea17df33-7476-412b-98a1-f879db01b59b"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"

```

[illegible]

Пример проверки ЭП (см. п. 3.3.11):

&lt;?xml version="1.0" encoding="UTF-8" standalone="yes"?&gt;



```
<VerifyRequest RequestID="594a2b5e-ed7b-413a-b9eb-2a649f891494">
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns2="http://commontypes.dss.signalcom.ru/" xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <OptionalInputs>
    <AccessToken>b976d95f-012a-4a4b-a2c6-fa5e913f1555</AccessToken>
  </OptionalInputs>
  <InputDocument>
    <ns2:Document>
      <ns2:Base64Data>MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkw</ns2:Base64Data>
    </ns2:Document>
  </InputDocument>
  <SignatureObject>
    <ns2:Base64Signature
Type="CMS">MIAGCSqGSIb3DQEHAqCAMIACAQExDjAMBggqhQMHAQECAgUAMIAGCSq
GSIB3DQEHAQAaOIIeZzCCBGMwggQQoAMCAQICCG7AkM8ATcCVmQwCgYIKoUDBwEB
AwIwZzELMAkGA1UEBhMCUIUxDzANBgNVBAcMBk1vc2NvdzEXMBUGA1UECgwOU2lnbm
FsLUNPTSBKU0MxLjAsBgNVBAMMJWUtTm90YXJ5IFRlc3QgQ0EgKEdPU1RSMzQxMC0yMD
EyLTl1NikwHhcNMjIwNDIyMTAyNDAA2WhcNMjIxMDIyMTAyNDAA2WjBmMQswCQYDVQQG
EwJSVTEvMC0GA1UEAwwm0JJqStCw0L3QtCyINCyOLLQsNC9INCyOLLQsNC9OL7QstC40Yc
xJjAkBgkqhkiG9w0BCQEWF3kua2ludHNvdkBzaWduYWwtY29tLnJlMGYwHwYIKoUDBwEBA
QEwEwYHKoUDAglKAAYIKoUDBwEBAgIDQwAEQAk7RIX8VZMhZGCzLLOPOEiLCyoiSaMO
UDJzHUw3LVDAncstMbfb3wHKYuhfo06S3WnARcwn7GzVsiA6VzpSznoJggKWMIICkjAMBgNV
HRMBAf8EAJAAMB0GA1UdDgQWBbTHwEcIZFvrjHselQ7omPehv48ZRTCBmAyDVR0jBIGQ
MIGNgBQvvbNAhB0yyQSfgYTNNdm56n/tKFrpGkwZzELMAkGA1UEBhMCUIUxDzANBgNVB
AcMBk1vc2NvdzEXMBUGA1UECgwOU2lnbmFsLUNPTSBKU0MxLjAsBgNVBAMMJWUtTm90
YXJ5IFRlc3QgQ0EgKEdPU1RSMzQxMC0yMDEyLTl1NimCCAG7AQEBNwEBMB0GA1UdJQQ
WMBQGCCsGAQUFBwMCBggrBgEFBQCDBDBCbgNVHR8EOzA5MDegNaAZhjFodHRwOi8vd3
d3LmUtbn90YXJ5Lnl1L2Nybf90ZXN0L2Nybf9nmjAxMi0yNTYuY3JsMdcGCCsGAQUFBwEB
BCswKTAnBggrBgEFBQcwAYYYbaHR0cDovL29jc3B0ZXN0LmUtbn90YXJ5Lnl1MCgGBSsqFA2R
vBB8MHdCh0JRQl9CYICJTAWduYWwtQ09NIEpDUCAzLjEiMBMGA1UdIAQMMAowCAYGKo
UDZHEBMIGvBgUqhQNkcASBPtCBogwT0KHQmtCX0JggIkNBRElgMi4xIgwc0J/QkNCaINCjOK
YgIk5vdGFyeS1QUk8gMi41Igw30JfQsNC60LvRjtGH0LXQvdC40LUg4oS WIDE0OS8zLzIvMi0xO
DY4INC+0YIgmTQuMDguMjAxOQw00JfQsNC60LvRjtGH0LXQvdC40LUg4oS WIDE0OS83LzYt
MTE0INC+0YIgmJcuMDMuMjAyMDArBgNVHRAEJDAAigA8yMDIyMDQyNjEwMjQwNlQBDzIw
MjIwODI0MTAyNDAA2WjAOBgNVHQ8BAf8EBAMCA/gwCgYIKoUDBwEBAAwIDQQAIVM5c43
6960EQ9TkMuE+Om/lDK1FsKlxDLgvXvzNU13A+ArspiXEqlrEs3dj9/I0zhCbsvI7/PeW+KIRudfho
CMYICEDCCAgwCAQEwdTBnMQswCQYDVQQGEwJSVTEPMA0GA1UEBwwGTW9zY293MR
cwFQYDVQQKDA5TAWduYWwtQ09NIEpTQzEuMCwGA1UEAwwlZS1Ob3RhcnkgVG VzdCBDO
SAOR09TVFlzNDEwLTIwMTItMjU2KQIKAbsCQzwBNwJWZDAMBggqhQMHAQECAgUAoIIB
MDAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqsGSIB3DQEJBTEPFw0yMjA0MjYx
MjQwMTNaMC8GCSqsGSIB3DQEJBDEiBCCgAqmKN5seSWALooRNkJHAY5K7w44n1y4h0VLU
D4ekuTCBxAYLKoZIhvcNAQkQAi8xbGwgbEwg4wgaswDAYIKoUDBwEBAGIFAAGC9IUU0
u4tXLJwYfcRGARyp5FFXxLslquHJIAoPUWPYYweTBrpGkwZzELMAkGA1UEBhMCUIUxDzAN
BgNVBAcMBk1vc2NvdzEXMBUGA1UECgwOU2lnbmFsLUNPTSBKU0MxLjAsBgNVBAMMJW
UtTm90YXJ5IFRlc3QgQ0EgKEdPU1RSMzQxMC0yMDEyLTl1NikCCG7AkM8ATcCVmQwDAY
IKoUDBwEBAQEFAARAVDVuklrnaTWttjRIzVD9KNtHTASffTVR5dTIIittPfYOk6k4T32OQB/7aH
APT8kBMAR87MurTfEaMBFo6gUhRugAAAAAAAA==</ns2:Base64Signature>
  </SignatureObject>
  <ReturnVerificationReport/>
</VerifyRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VerifyResponse RequestID="594a2b5e-ed7b-413a-b9eb-2a649f891494"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns3="http://verificationreport.dss.signalcom.ru/">
```

c=RU</ns3:Subject>  
<ns3:Issuer>cn=e-Notary Test CA (GOSTR3410-2012-256), o=Signal-COM JSC,  
l=Moscow, c=RU</ns3:Issuer>

Пример зашифрования данных в формате CMS (см. п. 3.3.14):

```
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
```

<ns3:X509Certificate>MIID5jCCA5OgAwIBAgIKAbsCRRgBNwJXFjAKBggqhQMAHQED  
AjbBnMQswCQYDVQQGEwJSVTEPMA0GA1UEBwwGTW9zY293MRcwFQYDVQKDA5TaWd  
uYWwtQ09NIEpTQzEuMCwGA1UEAwwlZS10b3RhcnkG VGvzdCBDQSAoR09TVFIlzNDEwLTIw  
MTItMjU2KTAeFw0yMjA4MDgxNDU5MzZaFw0yMzAyMDQxNDU5MzZaMCgx CzAJBgNVBAY  
TAIjVMRkwFwYDVQQDDDBBQSOlQUk8tNjJwIHRlc3QzMGYwHwYIKoUDBwEBAQEwEwYHK  
oUDAgIkAAAYIKoUDBwEBAgIDQwAEQJJN/NQrvSGH395zRzjKPXnjaOB9sqe208cuQYAYUw7H  
HylXC80LRifhqIFny46+aloL+CKIPCsmTqR7q/eU9hSjggJXMIICUzAMBgNVHRMBAf8EAjAAM  
B0GA1UdDgQWBbTVEbXgRrltCwEBkpDSRj8daLcFyTCBmA YDVR0jBIGQMIGNgBQvvnNAhB  
0yyQSfgyTNQNdm56n/tKFrpGkwZzELMAkGA1UEBhMCUUIUxDzANBgNVBACMBk1vc2NvdzEX  
MBUGA1UECgwOU2lnbmFsLUNPTSBKU0MxLjAsBgNVBAMMJWUtTm90YXJ5IFRlc3QgQ0Eg  
KEdPU1RSMzQxMC0yMDEyLTI1NimCCAG7AQEBNwEBMB0GA1UdJQQWMBQGCCCCGAQUF  
BwMCBggrBgEFBQcDBDBCBgNVHR8EOzA5MDegNaAzhjFodHRwOi8vd3d3LmUtbm90YXJ5LjN  
J1L2Nybf90ZXN0L2Nybf9nMjA4MjUyYU9Y3JSMdC GCCsGAQUFBwEBBCCswKTANBggrBgEF  
BQcwAYYbaHR0cDovL29jc3B0ZXN0LmUtbm90YXJ5LjNjA1MIGvBgUqhQnkcASBpTCBogwT0K  
HqmtCX0JggIkNBREIgmI4xIgcwOJ/QkNCaINCjOKYJgk15vdGFyeS1QUk8gmI44Igw30JfQsNC60L  
vRjtGH0LXQvdC40LUg4oS WIDE00S8zLzIvMi0xODY4INC+0YIgmTQuMDguMjA4XOQw00fJQsN  
C60LvRjtGH0LXQvdC40LUg4oS WIDE00S83LzYtMTE0INC+0YIgmJcuMDMuMjA4YMDArBgNV  
HRAEJDAigA8yMDIyMDgwODE0NTkzNlQBDzIwMjJlMjA2MTQ1OTM2WjA0BGNVHQ8BAf8E  
BAMCA/gwCgYIKoUDBwEBAwIDQQA LswISXehnp8K523Qhgv2UgyAx6CguFlci45m9IfoiQMY  
IwlbMD5kSihJ4p87uZqHJjXxmZGYyQ7DbvEERq5W</ns3:X509Certificate>

Пример расшифрования данных в формате CMS с подтверждением операции (см. п. 3.3.15). В ответе на первый запрос расшифрования данных возвращается идентификатор транзакции, который необходимо использовать для подтверждения операции расшифрования (см. п. 6.1.3):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <DecryptRequest RequestID="451fde09-9bcd-47e8-8ee9-74e5e49fcc54"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
    <OptionalInputs>
      <AccessToken>ca7e67c0-a018-4e88-9311-27f1e2fba2cb</AccessToken>
    </OptionalInputs>
    <InputDocument Name="document.p7e">
      <ns2:Document>
        <ns2:Base64Data MimeTypes="application/pkcs7-mime; smime-type=enveloped-
data">MIAGCSqGSIb3DQEHA6CAMIACAQAxggFOMIIBSgIBADB1MGcx CzAJBgNVBAYTAIJ
VMQ8wDQYDVQQHDAZNb3Njb3cx FzAVBgNVBAoMDINpZ25hbC1DT00gSINDMS4wLAYDV
QQDDC VILU5vdGFYeSBUXZN0IENBICHT1NUUjM0MTAtMjAxMi0yNTYpAgoBuwJFGAE3AI
cWMB8GCCqFAw cBAQE BMBMGBByqFAwICJAAGCCqFAw cBAQICBIGsMIGpMCgEIKC1J6QR
Ac1rhQUvSIGSc0gKLdsQTf1bK+ybkU5lq1A4BAQ0bT+hoH0GCSqFAw cBAGUBAaBmMB8GCCq
FAw cBAQE BMBMGBByqFAwICJAAGCCqFAw cBAQICA0MABEB2HZ0fBTXVEPJemKm0vyKW
X+33abdLhDp1n+eS+q37SCMuEtfoQfxNWSYtpvZ5SdUBL1NkL43QhbsT5xGFHYFZBAhhdqjMhs
loRDCABgkqhkiG9w0BBwEwHwYGGKouDAGIVMBUECL7WpZf/YqqnBgkqhQMHAQIFAQGggA
Q8qkH1xq0TgFK1NEPPfscn3YQKEvwxSqoouEdNzn5x2EtezgYr1ZhBWOHkbMVtuTsyiNjNBn0P
MQmcdv5AAAAAAAAAAAAAAAAAA==</ns2:Base64Data>
      </ns2:Document>
    </InputDocument>
    <EncryptionType>CMS</EncryptionType>
  </DecryptRequest>

  <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
  <DecryptResponse RequestID="451fde09-9bcd-47e8-8ee9-74e5e49fcc54"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
```

```
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <Result>
    <ResultMajor>Success</ResultMajor>
    <ResultMinor>ConfirmationRequired</ResultMinor>
  </Result>
  <OptionalOutputs>
    <TransactionID>99549686</TransactionID>
  </OptionalOutputs>
</DecryptResponse>
```

После подтверждения операции расшифрования посылается второй запрос на расшифрование данных с ограниченным набором параметров (маркер доступа и идентификатор транзакции), в ответе на запрос возвращаются расшифрованные данные:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DecryptRequest RequestID="61e23e44-d1d5-47fa-819f-bed5fc52a667"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <OptionalInputs>
    <AccessToken>ca7e67c0-a018-4e88-9311-27f1e2fba2cb</AccessToken>
    <TransactionID>99549686</TransactionID>
  </OptionalInputs>
</DecryptRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DecryptResponse RequestID="61e23e44-d1d5-47fa-819f-bed5fc52a667"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <Result>
    <ResultMajor>Success</ResultMajor>
    <ResultMinor>OperationCompleted</ResultMinor>
  </Result>
  <OutputDocument>
    <ns2:Base64Data>MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTIzNDU2Nz
g5MDEyMzQ1Njc4OTAxMjM0NTY3ODkw</ns2:Base64Data>
  </OutputDocument>
</DecryptResponse>
```

Пример создания невидимой ЭП документа в формате PDF:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignRequest RequestID="50170bfe-19c7-4e82-8d46-dbbe19b68d20"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commontypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <OptionalInputs>
    <AccessToken>25c5f04d-03f2-4da9-966b-f0de1654ee75</AccessToken>
  </OptionalInputs>
  <InputDocument Name="document.pdf">
    <ns2:Document>
      <ns2:Base64Data>JVBERi0xLjUN...</ns2:Base64Data>
    </ns2:Document>
  </InputDocument>
  <SignatureType>PADES</SignatureType>
  <SignParameters>
```

```

<ns2:PDFSignParameters>
  <ns2:Name>Name</ns2:Name>
  <ns2:Reason>Reason</ns2:Reason>
  <ns2:Location>Location</ns2:Location>
  <ns2:ContactInfo>ContactInfo</ns2:ContactInfo>
</ns2:PDFSignParameters>
</SignParameters>
<KeySelector>
  <ns2:KeyName>gost2012-256</ns2:KeyName>
</KeySelector>
<AddTimestamp/>
</SignRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignResponse RequestID="50170bfe-19c7-4e82-8d46-dbbe19b68d20"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commonypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <Result>
    <ResultMajor>Success</ResultMajor>
    <ResultMinor>OperationCompleted</ResultMinor>
  </Result>
  <SignatureObject>
    <ns2:Base64Signature>JVBERi0xLjUN...</ns2:Base64Signature>
  </SignatureObject>
</SignResponse>

```

Пример создания видимой сертифицирующей ЭП документа в формате PDF:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignRequest RequestID="2a326ca6-82ce-499c-935c-5b53dc55f1bc"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commonypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <OptionalInputs>
    <AccessToken>8d95a761-ef68-41d5-81f3-24cb78ffcac4</AccessToken>
  </OptionalInputs>
  <InputDocument Name="document.pdf">
    <ns2:Document>
      <ns2:Base64Data>JVBERi0xLjUN...</ns2:Base64Data>
    </ns2:Document>
  </InputDocument>
  <SignatureType>PADES</SignatureType>
  <SignParameters>
    <ns2:PDFSignParameters>
      <ns2:Name>Name</ns2:Name>
      <ns2:Reason>Reason</ns2:Reason>
      <ns2:Location>Location</ns2:Location>
      <ns2:ContactInfo>ContactInfo</ns2:ContactInfo>
      <ns2:DocMDP P="1"/>
      <ns2:VisibleSignature>
        <ns2:BottomTextSignature>
          <ns2:Alignment>Center</ns2:Alignment>
          <ns2:Rectangle Space="20" Width="160" Height="50"/>
          <ns2:Border Width="2.0">
            <ns2:Color Red="0" Green="0" Blue="255"/>
          </ns2:Border>
          <ns2:Background>
            <ns2:Color Red="255" Green="255" Blue="255"/>
          </ns2:Background>
        </ns2:BottomTextSignature>
      </ns2:VisibleSignature>
    </ns2:PDFSignParameters>
  </SignParameters>
</SignRequest>

```

```
</ns2:Background>
<ns2:Text Leading="1.5">
  <ns2:Color Red="0" Green="0" Blue="255"/>
  <ns2:Font Size="6.0">
    <ns2:Name>Roboto-Bold</ns2:Name>
  </ns2:Font>
</ns2:Text>
</ns2:BottomTextSignature>
</ns2:VisibleSignature>
</ns2:PDFSignParameters>
</SignParameters>
<KeySelector>
  <ns2:KeyName> gost2012-256</ns2:KeyName>
</KeySelector>
<AddTimestamp/>
</SignRequest>

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<SignResponse RequestID="2a326ca6-82ce-499c-935c-5b53dc55f1bc"
xmlns="http://api.customer.dss.signalcom.ru/" xmlns:ns6="http://verificationreport.dss.signalcom.ru/"
xmlns:ns5="http://www.w3.org/2001/04/xmlenc#" xmlns:ns2="http://commonypes.dss.signalcom.ru/"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <Result>
    <ResultMajor>Success</ResultMajor>
    <ResultMinor>OperationCompleted</ResultMinor>
  </Result>
  <SignatureObject>
    <ns2:Base64Signature>JVBERi0xLjUN...</ns2:Base64Signature>
  </SignatureObject>
</SignResponse>
```

## ЛИТЕРАТУРА

1. SOAP Version 1.2, W3C Recommendation, 27 April 2007.
2. Housley, R., Cryptographic Message Syntax, RFC 5652, September 2009.
3. DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0. OASIS, 12 November 2010.
4. XML Signature Syntax and Processing (Second Edition). W3C Recommendation, 10 June 2008.
5. D. Pinkas, N. Pope, J. Ross, CMS Advanced Electronic Signatures (CAvES). RFC 5126, February 2008.
6. XML Path Language (XPath) Version 1.0. W3C Recommendation, 16 November 1999.
7. PKCS #10 v1.7: Certification Request Syntax Standard. RSA Laboratories, May 26, 2000.
8. J. Schaad, M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, June 2008.
9. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
10. Housley, R., Polk, W., Ford, W. and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.
11. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. V.Popov, I.Kurepkin, S.Leontiev, RFC 4357, January 2006.
12. Р 1323565.1.023-2018. «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509». Федеральное агентство по техническому регулированию и метрологии, 2018.
13. Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии, 2016.
14. МР 26.2.002-213. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS. Методические рекомендации. Технический комитет по стандартизации «Криптографическая защита информации», 2013.
15. Р 1323565.1.033-2020. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 26 «Криптографическая защита информации», 2020.
16. C. Adams, P. Cain, D. Pinkas, R. Zuccherato, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, August 2001.
17. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
18. K. Zeilenga, Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names, RFC 4514, June 2006.
19. Signal-COM DSS Server. Руководство программиста. ШКНР.00042-01 33 01. ЗАО «Сигнал-КОМ», 2017.
20. Signal-COM Cloud DSS. Руководство системного программиста. ШКНР.00051-01 32 01. АО «СИГНАЛ-КОМ», 2021.

- 
21. Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0. OASIS, 11 April 2007.
  22. D. Hardt, The OAuth 2.0 Authorization Framework, RFC 6749, October 2012.
  23. Параметры эллиптических кривых для криптографических алгоритмов и протоколов. Методические рекомендации ТК 26, МР 26.2.002-2018. Технический комитет по стандартизации «Криптографическая защита информации», 2018.
  24. D. M'Raihi, S. Machani, M. Pei, J. Rydell, TOTP: Time-Based One-Time Password Algorithm, RFC 6238, May 2011.
  25. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen, HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226, December 2005.
  26. OASIS Standard, WS-Trust 1.3, 19 March 2007.
  27. OASIS Standard, WS-Trust 1.4, 2 February 2009.
  28. OASIS Standard, OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), March 2004.
  29. OASIS Standard, Web Services Security Username Token Profile Version 1.1.1, 18 May 2012.
  30. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
  31. ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. European Telecommunications Standards Institute ETSI.
  32. ECMA-376. Office Open XML file formats, 4th edition, December 2012. Ecma International.
  33. Федеральный закон № 63-ФЗ от 06.04.2011 «Об электронной подписи».