

Единая система электронной подписи

Описание программы

Листов 32

Москва
2020

АННОТАЦИЯ

В данном программном документе приведено описание прикладного программного обеспечения Единой системы электронной подписи (ЕСЭП).

СОДЕРЖАНИЕ

| | |
|--|----|
| Аннотация..... | 2 |
| Перечень терминов, сокращений и обозначений | 5 |
| 1 Общие сведения..... | 6 |
| 1.1 Обозначение и наименование программы | 6 |
| 1.2 Программное обеспечение, необходимое для функционирования программы | 6 |
| 1.2.1 Требования к программному обеспечению АРМ | 6 |
| 1.2.2 Требования к программному обеспечению серверных групп | 6 |
| 1.3 Языки программирования, на которых написана программа | 7 |
| 2 Функциональное назначение..... | 7 |
| 2.1 Назначение программы | 7 |
| 2.2 Сведения о функциональных ограничениях на применение | 8 |
| 3 Описание логической структуры..... | 8 |
| 3.1 Алгоритм Системы..... | 8 |
| 3.2 Используемые методы..... | 9 |
| 3.3 Структура Системы..... | 9 |
| 3.4 Связи программы с другими программами | 10 |
| 4 Используемые технические средства..... | 11 |
| 4.1 Требования к техническим средствам АРМ | 11 |
| 4.2 Требования к серверным аппаратным средствам..... | 12 |
| 5 Вызов и загрузка..... | 12 |
| 6 Входные и выходные данные | 13 |
| 6.1 Формат взаимодействия ЕСЭП с Внешней системой | 13 |
| 6.2 Описание методов ЕСЭП..... | 13 |
| 6.3 Сервис работы с файлами | 15 |
| 6.3.1 Метод CountImages «Получение количества страниц изображения файла» | 15 |
| 6.3.2 Метод DownloadFileEx «Выгрузка файла из Сервиса создания ЭП, включая отсоединенные ЭП» | 15 |
| 6.3.3 Метод GetFileDescription «Возвращение описания файла»..... | 15 |
| 6.3.4 Метод GetImage «Получение требуемой страницы изображения файла»..... | 16 |
| 6.3.5 Метод UploadFileV3 «Загрузка файла в Сервис создания ЭП» | 17 |
| 6.4 Сервис визуализации и электронного подписания | 17 |
| 6.4.1 Метод AddSignatureTimestamp «Добавление штампа времени к CMS подписи» | 17 |

| | | |
|--------|---|----|
| 6.4.2 | Метод CreateUIToShowDocuments «Формирование пользовательского интерфейса просмотра подписанных ЭП документов»..... | 18 |
| 6.4.3 | Метод CreateUIToShowSignatures «Формирование пользовательского интерфейса для просмотра информации о наложенных ЭП»..... | 18 |
| 6.4.4 | Метод CreateUIToSignDocument «Формирование пользовательского интерфейса просмотра и подписания документа клиентской ЭП с фиксацией типа подписываемого документа» | 19 |
| 6.4.5 | Метод CreateUIToSignV7 «Формирование пользовательского интерфейса просмотра и подписания файлов клиентской ЭП» | 20 |
| 6.4.6 | Метод GetCertificateInfo «Возвращение информации о сертификате» | 21 |
| 6.4.7 | Метод GetFileCertificatesUserInfo «Возвращение информации об сертификатах, которыми подписан файл» | 22 |
| 6.4.8 | Метод GetFileSignatureInfo «Возвращение информации об ЭП, наложенных на файл» | 22 |
| 6.4.9 | Метод GetOperationInfo «Возвращение информации об операции» | 23 |
| 6.4.10 | Метод GetOperationState «Возвращение информации о статусе операции»..... | 24 |
| 6.4.11 | Метод GetOriginal «Формирование копии файла без наложенных подписей».. | 24 |
| 6.4.12 | Метод GetSignatureExistenceInfo «Проверка наличия ЭП на файлах» | 25 |
| 6.4.13 | Метод AttachSignature «Присоединение подписи к данным»..... | 25 |
| 6.4.14 | Метод DetachSignature «Отсоединение данных от подписи» | 26 |
| 6.4.15 | Метод GetSupportedAlgorithms «Список поддерживаемых алгоритмов ЭП».... | 26 |
| 6.5 | Описание общих структур данных..... | 27 |

ПЕРЕЧЕНЬ ТЕРМИНОВ, СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В текст документа введены следующие специальные обозначения.

Таблица 1 – Принятые в документе специальные обозначения и их описание

| Обозначение | Описание |
|--------------------|---|
| ЕСЭП | Единая система электронной подписи |
| Пользователь | Лицо, имеющее доступ к данным Внешней системы |

В настоящий документ введены следующие специальные сокращения на русском и английском языках.

Таблица 2 – Принятые в документе специальные сокращения и их определения

| Сокращение | Определение |
|-------------------|--|
| SQL | Structured query language (рус.язык структурированных запросов) |
| TCP/IP | Transmission Control Protocol/Internet Protocol (рус. протокол управления передачей/межсетевой протокол) |
| АРМ | Автоматизированное рабочее место |
| ГОСТ | Государственный стандарт |
| ИБП | Источник бесперебойного питания |
| НЖМД | Накопитель на жёстких магнитных дисках |
| ПК | Персональный компьютер |
| СУБД | Система управления базами данных |
| ЭВМ | Электронная вычислительная машина |

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование программы

Полное наименование: Единая система электронной подписи.

Краткое наименование: ЕСЭП, Система.

1.2 Программное обеспечение, необходимое для функционирования программы

1.2.1 Требования к программному обеспечению АРМ

Таблица 3 содержит требования к программному обеспечению АРМ.

Таблица 3 – Требования к программному обеспечению АРМ

| Наименование | Характеристика |
|-------------------|---|
| ОС | Семейства Windows |
| Web-браузер | Internet Explorer версии не ниже 11.0; Mozilla Firefox версии не ниже 76; Opera версии не ниже 66.0; Google Chrome версии не ниже 83.0; Яндекс Браузер версии не ниже 20.0. |
| Ключевой носитель | eToken ГОСТ (форм-фактор «USB-ключ»); RuToken ЭЦП (форм-фактор «USB-ключ»); JaCarta ГОСТ 2.0. Работа с ключевыми носителями RuToken производится через специальное ПО от компании-поставщика ключевого носителя. |
| Криптопровайдер | КриптоПро CSP, VipNet CSP, Signal-COM CSP, Lissi CSP, AvCSP |

1.2.2 Требования к программному обеспечению серверных групп

Минимальные требования к составу программно-аппаратных средств отображены ниже:

- веб-сервер:
 - аппаратное обеспечение:
 - 64-разрядный четырехъядерный процессор с тактовой частотой не менее 2 ГГц;
 - ОЗУ не менее 8 Гб;
 - ПЗУ не менее 100 Гб SAS HDD 15000 Rpm.
 - операционная система Microsoft Windows Server 2012;

- программное обеспечение Microsoft .NET Framework 4.8, КриптоПро CSP;
- программное обеспечение для размещения веб-приложений Microsoft IIS 8.0.
- сервер баз данных:
 - аппаратное обеспечение:
 - 64-разрядный четырехъядерный процессор с тактовой частотой не менее 2 ГГц;
 - ОЗУ не менее 16 Гб;
 - ПЗУ не менее 200 Гб SAS HDD 15000 Rpm.
 - операционная система: Microsoft Windows Server 2012;
 - программное обеспечение: MS SQL Server 2012.

Локальная вычислительная сеть Заказчика должна обеспечивать канал связи между рабочими станциями и сервером базы данных с пропускной способностью не ниже 100 Мбит/с.

С целью достижения требований по обеспечению производительности необходимо реализовать состав программно-аппаратных средств в соответствии с характеристиками, указанными в разделе 4.2.

1.3 Языки программирования, на которых написана программа

Исходным языком программирования Системы является С#. Среда разработки – Microsoft Visual Studio 2019.

Интерфейс пользователя разработан с использованием технологии HTML, JavaScript, MVC, AJAX. Среда разработки – Microsoft Visual Studio 2019.

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Назначение программы

Назначением ЕСЭП является:

- обеспечение выполнения процедуры подписания электронных документов усиленной квалифицированной электронной подписью в соответствии с Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», постановлением Правительства Российской Федерации от 09.02.2012 № 111 «Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее

- использования, а также об установлении требований к обеспечению совместимости средств электронной подписи», приказом ФСБ РФ от 27.12.2011 N 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;
- обеспечение выполнения процедур проверки и подтверждения подписанных электронных документов;
 - предоставление возможности временного защищенного хранения подписанных электронных документов и доступа к электронным документам по запросу Внешней системы.

2.2 Сведения о функциональных ограничениях на применение

Сведения о функциональных ограничениях на применение приведен в разделе 1.2.2.

3 ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1 Алгоритм Системы

Система предназначена для обеспечения возможности использования усиленной квалифицированной подписи при подписании электронных документов для придания им юридической значимости.

ЕСЭП обеспечивает выполнение следующих основных процессов:

- преобразование электронного документа в файлы графических форматов;
- формирование и предоставление пользовательского интерфейса предварительного просмотра и подписания электронного документа;
- формирование отсоединенной или присоединенной усиленной квалифицированной подписи на электронном документе;
- улучшение подписи, посредством наложения штампа времени;
- предоставление результата подписи.

Порядок взаимодействия внешней информационной системы с ЕСЭП осуществляется с помощью веб-сервисов загрузки и подписания файла:

- Внешняя система загружает в ЕСЭП файл для подписания, используя метод UploadFileV3 сервиса работы с файлами, и получает код доступа к загруженному файлу;
- для инициации подписания файла пользователем, Внешняя система вызывает метод CreateUIToSignV7 сервиса визуализации и электронного

подписания, которому передает необходимые параметры и полученный код доступа к загруженному файлу (файлам). В ответ внешняя ИС получает URL и идентификатор операции;

- Внешняя система открывает в браузере полученный URL, где пользователь просматривает и подписывает загруженный файл;
- после подписания файла пользователем, ЕСЭП может выполнить переход на заданный внешней ИС URL;
- используя метод DownloadFileEx сервиса работы с файлами, Внешняя система скачивает подписанный файл.

3.2 Используемые методы

Система создана с использованием языка программирования С#. В основу реализации Системы положены методы, определяемые выбранными для разработки средствами.

3.3 Структура Системы

В состав Системы входят следующие подсистемы:

- 1) подсистема проверки и наложения подписей;
- 2) модуль выполнения криптографических функций
- 3) подсистема ведения реестра удостоверяющих центров;
- 4) криптопровайдер.

Описание функций подсистем ЕСЭП приведено в Таблица 4. Все подсистемы в ходе функционирования используют единую базу данных.

Таблица 4. Описание функций подсистем

| № | Наименование и статус подсистемы | Описание функций подсистемы |
|----|---|---|
| 1. | Подсистема проверки и наложения подписей | Подсистема предназначена для: <ul style="list-style-type: none"> • обработки запросов, поступающих от внешних систем; • обеспечения проверки и подписания электронных документов; • координации и передачи запросов и ответов между подсистемами ЕСЭП. |
| 2. | Подсистема ведения реестра удостоверяющих | Подсистема предназначена для актуализации реестров доверенных удостоверяющих центров (УЦ), сертификатов, выданных доверенными УЦ, а также предоставления |

| № | Наименование и статус подсистемы | Описание функций подсистемы |
|----|----------------------------------|--|
| | центров | информации о состоянии сертификата на запрошенный момент времени. |
| 3. | Криптомодуль | Библиотека функций, реализующих базовые криптографические примитивы. |
| 4. | Криптопровайдер | Позволяет осуществлять криптографические операции. |

3.4 Связи программы с другими программами

Система взаимодействует со следующими системами:

- Электронный сервис проверки ЭП;
- Внешней системой;
- Доверенные службы штампов времени (TSP).

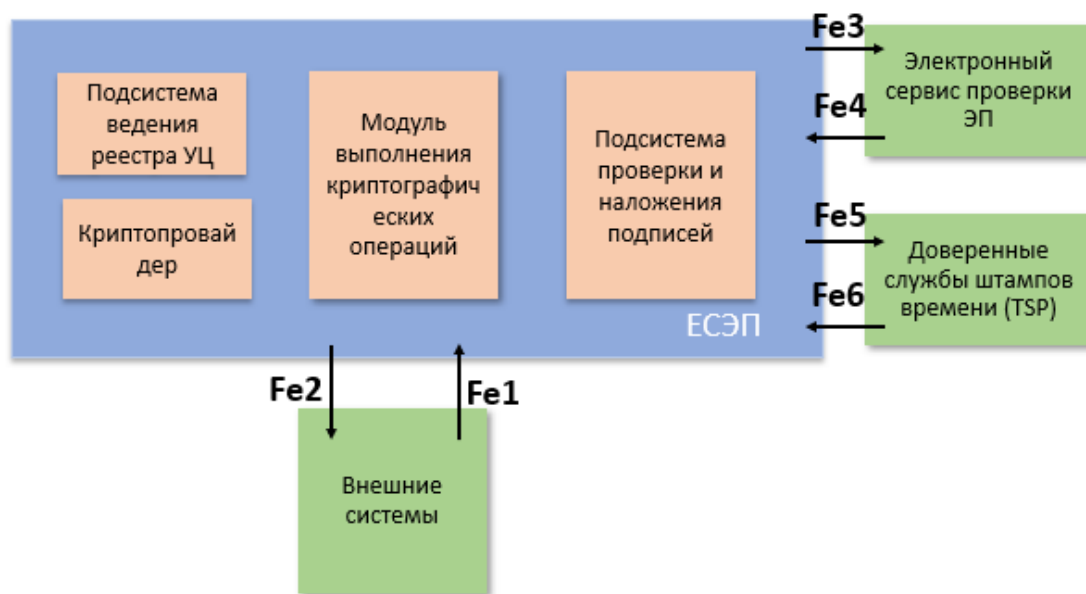


Рисунок 1 – Элементы архитектуры Сервиса создания ЭП

Таблица 5. Перечень информационных взаимодействий, представленных на Рисунке 1

| № | Описание |
|------------|---|
| Fe1 | Запрос на подписание документов ЭП |
| Fe2 | Передача подписанных документов ЭП |
| Fe3 | Запрос на проверку ЭП и полномочий |
| Fe4 | Получение информации о проверке ЭП и полномочий |
| Fe5 | Запрос информации от службы штампов времени |
| Fe6 | Метка времени |

Программно-технические средства доработанной Системы соответствуют стандартам сети Интернет и поддерживают прием-передачу данных по протоколу TCP/IP.

Физический сервер, на котором размещаются программные компоненты Системы, имеет постоянное подключение к Интернет по протоколам TCP/IP.

Информационное взаимодействие между компонентами Системы осуществляется посредством доступа к единому хранилищу данных (СУБД).

Информационный обмен между компонентами Системы осуществляется без дополнительного вмешательства пользователя и без повторного ввода информации вручную.

Поступающая в Систему информация проходит необходимый контроль и корректировку до ввода в Систему.

Выходная информация из Системы поступает к пользователям посредством разработанного графического интерфейса пользователя.

4 ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

4.1 Требования к техническим средствам АРМ

Для автоматизированных рабочих мест пользователей используется рабочая станция в составе технических средств, представленных на Рисунок 2.

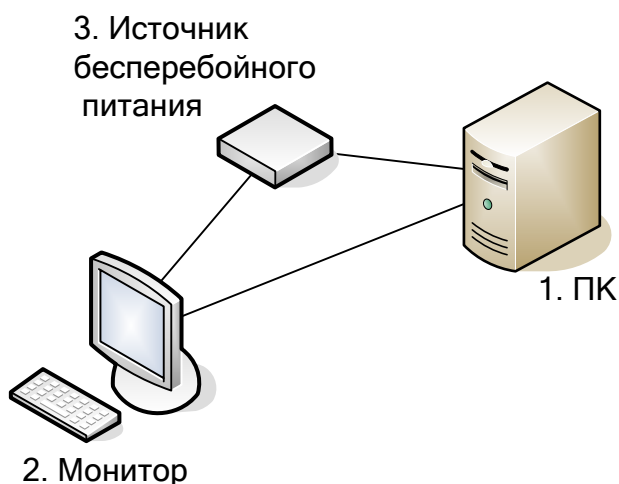


Рисунок 2 – Структурная схема технических средств АРМ

Источник бесперебойного питания в составе АРМ пользователя обеспечивает автономность от источников электропитания на время достаточное для безаварийного завершения работы. Кроме того, устройство должно защитить оборудование от перепадов напряжения, проникающих через электрические и телефонные линии, а также через линию локальной сети.

Таблица 6 содержит требования к аппаратной части АРМ.

Таблица 6 – Требования к аппаратной части АРМ

| Параметр | Значение |
|--|--|
| ЦПУ | Intel Pentium IV 1.2 ГГц и выше |
| ОЗУ | не менее 256 Мб |
| НЖМД | не менее 1 Гб |
| Видеоадаптер, поддерживающий видеорежим | разрешение не менее 1024x768 |
| Сетевой адаптер | 1 x Ethernet 10Base-T |
| Скорость подключения к серверной части | 2 Мбит/сек |
| ИБП | 30 минут работы в режиме отключенного электропитания |

4.2 Требования к серверным аппаратным средствам

Таблица 7 содержит описание конфигурации технических характеристик серверов для достижения оптимальной производительности.

Таблица 7 – Технические характеристики серверов

| Назначение ресурса | Количество | | | | |
|------------------------|------------|---------|---------------------|--------------------|--------------------------|
| | CPU (core) | RAM, Gb | Локальные диски, Gb | Сетевые интерфейсы | Интерфейсы сети хранения |
| Сервер приложений | 8 | 8 | 100Gb | 1x 1GbE | 1x 1GbE |
| Сервер приложений | 8 | 8 | 100Gb | 1x 1GbE | 1x 1GbE |
| Сервер приложений | 2 | 8 | 100Gb | 1x 1GbE | 1x 1GbE |
| Сервер баз данных | 16 | 16 | 200Gb | 1x 1GbE | 1x 1GbE |
| Балансировщик нагрузок | 2 | 2 | 20Gb | 1x 1GbE | 1x 1GbE |

5 ВЫЗОВ И ЗАГРУЗКА

Запуск ЕСЭП на сервере осуществляется при помощи запуска служб IIS операционной системы (автоматически).

Запуск ЕСЭП на клиентском рабочем месте осуществляется при помощи запуска браузера и указания адреса Системы в адресной строке браузера.

6 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

6.1 Формат взаимодействия ЕСЭП с Внешней системой

Взаимодействие Системы с Внешней системой выполняется посредством сервисов. Система предоставляет доступ к сервисам только внешним системам, зарегистрированным в реестре внешних систем.

Для обеспечения доступа Внешней системы к методам, предоставляемым Системой, реализован стандартный интерфейс программирования приложений (API). API обеспечивает доступ к следующим сервисам:

- формирование и предоставление в ответ на запрос Внешней системы пользовательского интерфейса просмотра и подписания ЭП документа (-ов), полученного (-ых) от Внешней системы;
- формирование ЭП для документа в ответ на запрос, поступивший от пользователя Внешней системы;
- формирование результатов проверки ЭП, ранее подписанного электронного документа;
- передача документа и его ЭП в файловое хранилище и получение от файлового хранилища ссылки для доступа к подписанному документу;
- передача Внешней системе ссылки для доступа к подписанному документу.

Форматы и протоколы данных при взаимодействии Системы с Внешней системой в XML, с использованием протоколов HTTP, HTTPS, SOAP.

Для временного хранения файлов, создаваемых в ходе обработки входящих от Внешней системы запросов, подсистема наложения подписей использует временное файловое хранилище. После завершения работы с временными файлами Система удаляет файлы из временного файлового хранилища.

При положительном результате подписания документа файлы из временного хранилища забираются Внешней системой и передаются на постоянное хранение во Внешнюю систему, после чего удаляются из временного хранилища.

Выходная информация для пользователей поступает из ЕСЭП посредством разработанного графического интерфейса пользователя.

6.2 Описание методов ЕСЭП

Перечень всех методов Сервиса создания ЭП, используемых для обеспечения выполнения работы Сервиса создания ЭП, представлен в таблице ниже (**Ошибка! Источник ссылки не найден.**).

Таблица 8. Перечень внутренних методов Сервиса создания ЭП

| № | Метод | Назначение |
|--|-----------------------------|---|
| Сервис работы с файлами | | |
| 1 | CountImages | Получает количество постраничных изображений документа |
| 2 | DownloadFileEx | Выгружает файл из Сервиса ЭП, включая отсоединённые подписи (при их наличии) |
| 3 | GetFileDescription | Возвращает описание файла |
| 4 | GetImage | Получает изображение требуемой страницы документа |
| 5 | UploadFileV3 | Загружает файл в Сервис ЭП |
| Сервис визуализации и электронного подписания | | |
| 1 | AddSignatureTimestamp | Добавляет штамп времени к CMS подписи |
| 2 | CreateUIToShowDocuments | Формирует пользовательский интерфейс просмотра подписанных ЭП документов |
| 3 | CreateUIToShowSignatures | Формирует пользовательский интерфейс для просмотра информации о наложенных ЭП |
| 4 | CreateUIToSignDocument | Формирует пользовательский интерфейс просмотра и подписания документа клиентской ЭП с фиксацией типа подписываемого документа |
| 5 | CreateUIToSignV7 | Формирует пользовательский интерфейс просмотра и подписания файлов клиентской ЭП |
| 6 | GetCertificateInfo | Возвращает информацию о сертификате |
| 7 | GetFileCertificatesUserInfo | Возвращает информацию о сертификатах, которыми подписан файл |
| 8 | GetFileSignatureInfo | Возвращает информацию об ЭП, наложенных на файл |
| 9 | GetOperationInfo | Возвращает информацию об операции |
| 10 | GetOperationState | Возвращает информацию о статусе операции |
| 11 | GetOriginal | Формирует копию файла без наложенных подписей |
| 12 | GetSignatureExistenceInfo | Проверяет наличие ЭП на файлах |
| 13 | AttachSignature | Выполняет присоединение данных к подписи |
| 14 | DetachSignature | Выполняет отсоединение данных от подписи |
| 15 | GetSupportedAlgorithms | Возвращает список поддерживаемых алгоритмов |

6.3 Сервис работы с файлами

6.3.1 Метод CountImages «Получение количества страниц изображения файла»

Входные данные: GetCountImagesRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileInfoId | Идентификатор файла, для которого необходимо получить количество страниц изображения | + | GUID | |

Выходные данные: GetCountImagesResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--|----------------|-----------------------|-------------|
| 1 | CountImages | Запрошенное количество страниц изображения | + | Int32 | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.3.2 Метод DownloadFileEx «Выгрузка файла из Сервиса создания ЭП, включая отсоединенные ЭП»

Входные данные: DownloadFileExRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCode | Код доступа к файлу, который необходимо выгрузить | + | String | |

Выходные данные: DownloadFileExResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------|----------------|-----------------------|-------------|
| 1 | File | Запрошенный файл | + | FileEx | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.3.3 Метод GetFileDescription «Возвращение описания файла»

Входные данные: GetFileDescriptionRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCode | Код доступа к файлу, для которого необходимо вернуть описание | + | String | |

Выходные данные: GetFileDescriptionResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------|----------------|-----------------------|-------------|
| 1 | Description | Описание файла | - | String | |
| 2 | Name | Имя файла | + | String | |
| 3 | RequestResult | Результат запроса | + | RequestResult | |

6.3.4 Метод GetImage «Получение требуемой страницы изображения файла»

Входные данные: GetBase64StringImageRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileInfoId | Идентификатор файла, для которого необходимо получить количество страниц изображения | + | GUID | |
| 3 | NumberImage | Номер страницы изображения | + | Int32 | |

Выходные данные: GetBase64StringImageResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|----------------------------------|----------------|-----------------------|-------------|
| 1 | ImageBase64 | Запрошенная страница изображения | + | ImageBase64 | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.3.5 Метод UploadFileV3 «Загрузка файла в Сервис создания ЭП»

Входные данные: UploadFileV3Request

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|--------------------|---|----------------|------------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | Description | Описание файла | - | String | |
| 3 | File | Файл, который необходимо загрузить | + | File | |
| 4 | StorageType | Тип хранилища для размещения файла | + | Временное хранилище | |
| 5 | DetachedSignatures | Массив отсоединенных подписей | - | DetachedSignature Ex[] | |

Выходные данные: UploadFileV3Response

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|----------------------------------|----------------|-----------------------|-------------|
| 1 | FileAccessCode | Код доступа к загруженному файлу | + | String | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.4 Сервис визуализации и электронного подписания

6.4.1 Метод AddSignatureTimestamp «Добавление штампа времени к CMS подписи»

Входные данные: AddSignatureTimestampRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | Signature | CMS подпись без штампа времени | + | String | Base64 |
| 3 | TspUrl | Адрес службы штампов времени | + | String | |

Выходные данные: AddSignatureTimestampResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|------------------------|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | Signature | CMS подпись со штампом | - | String | Base64 |

| | | | | | |
|--|--|---------|--|--|--|
| | | времени | | | |
|--|--|---------|--|--|--|

6.4.2 Метод CreateUIToShowDocuments «Формирование пользовательского интерфейса просмотра подписанных ЭП документов»

Входные данные: CreateUIToShowDocumentsRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCodes | Коды доступа к файлам | + | String[] | |
| 3 | ReturnUrl | Адрес, на который необходимо перенаправить пользователя после завершения работы | - | String | |

Выходные данные: CreateUIToShowDocumentsResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | Составной | |
| 2 | URL | Адрес, на который необходимо перенаправить пользователя для просмотра подписанных ЭП документов | + | String | |

6.4.3 Метод CreateUIToShowSignatures «Формирование пользовательского интерфейса для просмотра информации о наложенных ЭП»

Входные данные: CreateUIToShowSignaturesRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCodes | Коды доступа к файлам | + | String[] | |
| 3 | ReturnUrl | Адрес, на который необходимо перенаправить пользователя после завершения работы | - | String | |

Выходные данные: CreateUIToShowSignaturesResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | URL | Адрес, на который необходимо перенаправить пользователя для просмотра информации о наложенных ЭП | + | String | |

6.4.4 Метод CreateUIToSignDocument «Формирование пользовательского интерфейса просмотра и подписания документа клиентской ЭП с фиксацией типа подписываемого документа»

Входные данные: CreateUIToSignDocumentRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------------|---|----------------|-----------------------|-------------------------|
| 1 | ClientSignatureFormat | Формат клиентской подписи | + | ClientSignatureFormat | |
| 2 | ClientSignatureKind | Вид клиентской подписи | + | ClientSignatureKind | |
| 3 | ClientSigningMode | Способ подписания файлов пользователем | + | ClientSigningMode | |
| 4 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 5 | DocumentId | ID документа, для которого производится подписание | + | GUID | |
| 6 | FileAccessCodes | Коды доступа к файлам | + | String[] | |
| 7 | Oids | Список OID для проверки | + | String[] | |
| 8 | ReturnUrl | Адрес, на который необходимо перенаправить пользователя после завершения работы | - | String | |
| 9 | ServerSignatureFormat | Формат серверной | - | ServerSignatureFormat | |

| | | | | | |
|----|--------------------|---|---|---------|--|
| | | подписи | | | |
| 10 | ServerSignRequired | Признак необходимости наложения серверной подписи | + | Boolean | |

Выходные данные: CreateUIToSignDocumentResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------|
| 1 | OperationID | Уникальный идентификатор операции | + | String | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |
| 3 | URL | Адрес, на который необходимо перенаправить пользователя для подписания документов | + | String | |

6.4.5 Метод CreateUIToSignV7 «Формирование пользовательского интерфейса просмотра и подписания файлов клиентской ЭП»

Входные данные: CreateUIToSignV7Request

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------------|---|----------------|-----------------------|-------------------------|
| 1 | ClientSignatureFormat | Формат клиентской подписи | + | ClientSignatureFormat | |
| 2 | ClientSignatureKind | Вид клиентской подписи | + | ClientSignatureKind | |
| 3 | ClientSigningMode | Способ подписания файлов пользователем | + | ClientSigningMode | |
| 4 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 5 | FileAccessCodes | Коды доступа к файлам | + | String[] | |
| 6 | Oids | Список OID для проверки | + | String[] | |
| 7 | ReturnUrl | Адрес, на который необходимо перенаправить пользователя после | - | String | |

| | | | | | |
|----|------------------------|---|---|-----------------------|--|
| | | завершения работы | | | |
| 8 | ServerSignatureFormat | Формат серверной подписи | - | ServerSignatureFormat | CMS |
| 9 | ServerSignRequired | Признак необходимости наложения серверной подписи | - | Boolean | |
| 10 | SignatureAlgorithmOids | OID допустимых алгоритмов подписи | + | List<string> | |
| 11 | AddTimestamp | Флаг необходимости добавления метки времени | - | Boolean | Есть флаг не задан, необходимость добавления метки времени определяется настройками ЕСЭП |

Выходные данные: CreateUIToSignResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------|
| 1 | OperationId | Уникальный идентификатор операции | + | String | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |
| 3 | Url | Адрес, на который необходимо перенаправить пользователя для подписания документов | + | String | |

6.4.6 Метод GetCertificateInfo «Возвращение информации о сертификате»

Входные данные: GetCertificateInfoRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------------------|
| 1 | Content | Тело сертификата | + | Byte[] | |
| 2 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |

Выходные данные: GetCertificateInfoResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------------|----------------|-----------------------|-------------|
| 1 | Info | Информация о сертификате | | CertificateInfo | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.4.7 Метод GetFileCertificatesUserInfo «Возвращение информации об сертификатах, которыми подписан файл»**Входные данные: GetFileCertificatesUserInfoRequest**

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCodes | Коды доступа к файлам | + | String[] | |

Выходные данные: GetFileCertificatesUserInfoResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|--------------------------|---|----------------|---------------------------|-------------|
| 1 | FileCertificateUserInfos | Информация о сертификатах, которыми подписан файл | - | FileCertificateUserInfo[] | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.4.8 Метод GetFileSignatureInfo «Возвращение информации об ЭП, наложенных на файл»**Входные данные: GetFileSignatureInfoRequest**

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCodes | Коды доступа к файлам | + | String[] | |

Выходные данные: GetFileSignatureInfoResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|--------------------|---------------------------------------|----------------|-----------------------|-------------|
| 1 | FileSignatureInfos | Информация об ЭП, наложенных на файлы | | FileSignatureInfo[] | |

| | | | | | |
|---|---------------|-------------------|---|---------------|--|
| 2 | RequestResult | Результат запроса | + | RequestResult | |
|---|---------------|-------------------|---|---------------|--|

6.4.9 Метод GetOperationInfo «Возвращение информации об операции»

Входные данные: GetOperationInfoRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | OperationId | Идентификатор операции | + | String | |

Выходные данные: GetOperationInfoResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------------|---|----------------|-----------------------|---|
| 1 | ClientSignatureFormat | Формат клиентской подписи | + | ClientSignatureFormat | |
| 2 | ClientSignatureKind | Вид клиентской подписи | + | ClientSignatureKind | |
| 3 | ClientSigningMode | Способ подписания файлов пользователем | + | ClientSigningMode | |
| 4 | Files | Информация о файлах | + | OperationFileInfo | |
| 5 | RequestResult | Результат запроса | + | RequestResult | |
| 6 | ReturnUrl | Адрес, на который необходимо перенаправить пользователя после завершения работы | + | String | |
| 7 | Type | Тип выполняемой операции | + | OperationType | |
| 8 | ClientHashAlgorithm | Допустимый алгоритм расчета хеша | - | HashAlgorithmType [] | Устарел - использовать SignatureAlgorithmOids |

| | | | | | |
|---|------------------------|------------------------------------|---|--------------|--|
| | | и ЭП | | | |
| 9 | SignatureAlgorithmOids | OID допустимых алгоритмов подписи. | - | List<string> | |

6.4.10 Метод GetOperationState «Возвращение информации о статусе операции»

Входные данные: GetOperationStateRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | OperationId | Идентификатор операции | + | String | |

Выходные данные: GetOperationStateResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|--------------------|----------------|-----------------------|-------------|
| 1 | OperationState | Статус операции | + | OperationState | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.4.11 Метод GetOriginal «Формирование копии файла без наложенных подписей»

Входные данные: GetOriginalRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|--|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCode | Код доступа к файлу, для которого необходимо сформировать копию без подписей | + | String | |

Выходные данные: GetOriginalResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|-------------------------|----------------|-----------------------|-------------|
| 1 | FileAccessCode | Код доступа к файлу без | + | String | |

| | | | | | |
|---|---------------|-------------------|---|---------------|--|
| | | подписей | | | |
| 2 | RequestResult | Результат запроса | + | RequestResult | |

6.4.12 Метод GetSignatureExistenceInfo «Проверка наличия ЭП на файлах»

Входные данные: GetSignatureExistenceInfoRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCodes | Коды доступа к файлам | + | String[] | |

Выходные данные: GetSignatureExistenceInfoResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|-------------------------|-----------------------------------|----------------|--------------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | SignatureExistenceInfos | Информация о наличии ЭП на файлах | - | SignatureExistenceInfo[] | |

6.4.13 Метод AttachSignature «Присоединение подписи к данным»

Входные данные: AttachSignatureRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|--|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCode | Код доступа к файлу, к которому приложена в поле DetachedSignatures отсоединенная подпись. Отсоединенная подпись должна быть одна. | + | String | |

Выходные данные: AttachSignatureResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|-------------------------------|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | FileAccessCode | Код доступа к результирующему | + | String | |

| | | | | | |
|--|--|---|--|--|--|
| | | файлу, в котором данные присоединены к подписи. | | | |
|--|--|---|--|--|--|

6.4.14 Метод DetachSignature «Отсоединение данных от подписи»

Входные данные: DetachSignatureRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |
| 2 | FileAccessCode | Код доступа к файлу. Файл должен содержать подпись с присоединенными данными. | + | String | |

Выходные данные: DetachSignatureResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|--|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | FileAccessCode | Код доступа к результирующему файлу, в котором подпись отсоединена от файла и находится в поле DetachedSignatures. | + | String | |

6.4.15 Метод GetSupportedAlgorithms «Список поддерживаемых алгоритмов»

Входные данные: GetSupportedAlgorithmsRequest

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|---|----------------|-----------------------|-------------------------|
| 1 | Credentials | Реквизиты доступа к Сервису создания ЭП | + | Credentials | Логин/пароль внешней ИС |

Выходные данные: GetSupportedAlgorithmsResponse

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------------|--------------------|----------------|-----------------------|-------------|
| 1 | RequestResult | Результат запроса | + | RequestResult | |
| 2 | SignatureAlgorithmO | Список OID | + | List<String> | |

| | | | | |
|-----|------------------------------|--|--|--|
| ids | поддерживаемых алгоритмов ЭП | | | |
|-----|------------------------------|--|--|--|

6.5 Описание общих структур данных

1. Тип: Credentials

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|-----------------------|----------------|-----------------------|-------------|
| 1 | Login | Логин внешней системы | + | String | |
| 2 | Password | Пароль | + | String | |

2. Тип: RequestResult

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|------------------------------|----------------|-----------------------|--|
| 1 | ErrorCode | Код ошибки | - | String | |
| 2 | ErrorData | Данные ошибки | - | ErrorDataItem | |
| 3 | ErrorMessage | Описание ошибки | - | String | |
| 4 | WasSuccessful | Результат выполнения запроса | + | Boolean | TRUE, если запрос выполнен успешно, в противном случае – FALSE |

3. Тип: FileEx

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|--------------------|-----------------------|----------------|-------------------------|-------------|
| 1 | Body | Тело файла | + | Byte | |
| 2 | Info | Информация о файле | + | FileInfo | |
| 3 | DetachedSignatures | Отсоединенные подписи | - | DetachedSignature [] | |

4. Тип: CertificateInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------------|---------------------------------------|----------------|-----------------------|-------------|
| 1 | Algorithm | Алгоритм | + | String | |
| 2 | IsValid | Валидность | + | Boolean | |
| 3 | KeyUsages | Назначение ключа | + | String | |
| 4 | SerialNumber | Серийный номер | + | String | |
| 5 | SubjectKeyIdentifier | Идентификатор ключа | + | String | |
| 6 | ValidFrom | Начало периода валидности сертификата | + | Nullable<DateTime> | |
| 7 | ValidTo | Конец периода валидности сертификата | + | Nullable<DateTime> | |

5. Тип: FileCertificateUserInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------------|---------------------------|----------------|-----------------------|-------------|
| 1 | CertificatesUserInfo | Информация о сертификатах | + | CertificateUserInfo[] | |
| 2 | FileAccessCode | Код доступа к файлу | + | String | |
| 3 | FileInfo | Информация о файле | + | FileInfoEx | |

6. Тип: FileSignatureInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|-----------------------|----------------|-----------------------|-------------|
| 1 | FileAccessCode | Код доступа к файлу | + | String | |
| 2 | FileInfo | Информация о файле | + | FileInfoEx | |
| 3 | Signatures | Информация о подписях | + | SignatureInfo | |

7. Тип: OperationFileInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------|----------------|-----------------------|-------------|
| 1 | AccessCode | Код доступа | + | String | |
| 2 | Processed | | + | Boolean | |

8. Тип: SignatureExistenceInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|----------------|---------------------|----------------|-----------------------|-------------|
| 1 | Exists | Признак наличия ЭП | + | Boolean | |
| 2 | FileAccessCode | Код доступа к файлу | + | String | |

9. Тип: ErrorDataItem

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------|----------------|-----------------------|-------------|
| 1 | Key | Ключ | + | String | |
| 2 | Value | Значение | + | String | |

10. Тип: FileInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|-----------------------------|----------------|-----------------------|-------------|
| 1 | MimeType | Тип данных файла (MIME-тип) | + | String | |
| 2 | Name | Имя файла | + | String | |

11. Тип: CertificateUserInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|--------------------|----------------|-----------------------|-------------|
| 1 | CommonName | ФИО | + | String | |
| 2 | INN | ИНН | + | String | |
| 3 | OGRN | ОГРН | + | String | |

| | | | | | |
|---|----------|-----------------|---|--------------------|--|
| 4 | OGRNIP | ОГРНИП | + | String | |
| 5 | SignDate | Дата подписания | + | Nullable<DateTime> | |
| 6 | SNILS | СНИЛС | + | String | |

12. Тип: FileInfoEx

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения/Тип | Комментарий |
|---|---------------|-----------------------------|----------------|-----------------------|-------------|
| 1 | CreationDate | Дата создания | + | DateTime | |
| 2 | MimeType | Тип данных файла (MIME-тип) | + | String | |
| 3 | ModifiedDate | Дата изменения | + | DateTime | |
| 4 | Name | Имя файла | + | String | |
| 5 | Size | Размер в байтах | + | Int32 | |

13. Тип: SignatureInfo

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения /Тип | Комментарий |
|---|------------------------------|--|----------------|------------------------|---|
| 1 | CertificateThumbprint | Отпечаток ключа подписи (SHA-1) | + | String | |
| 2 | CertificateFingerPrintSha256 | Отпечаток сертификата подписанта (SHA-256) | + | String | |
| 3 | CertificationAuthority | Удостоверяющий центр | + | String | |
| 4 | ClientSignatureKind | Вид клиентской подписи | + | SignatureKind | Значение 1 – присоединенная Значение 2 – отсоединенная |
| 5 | ErrorMessage | Описание причины невалидности подписи | + | String | |
| 6 | FailReason | Причина некорректности подписи | + | Int32 | |
| 7 | IsValid | Признак корректности подписи | + | Boolean | |
| 8 | IsSignatureValid | Признак математической корректности подписи | - | Nullable<Boolean> | Может быть не задан если ошибка при проверке найдена до проверки на математическую корректность |
| 9 | IsCertificateValid | Признак валидности сертификата ключа подписи | - | Nullable<Boolean> | Может быть не задан если ошибка при проверке найдена до |

| | | | | | |
|--------|-----------------------------|---|---|-----------------------------|---|
| | | | | | проверки сертификата на валидность |
| 1 0 | Owner | Владелец | + | String | |
| 1 1 | CountryName | Страна | + | String | Двухсимвольный код страны по ISO 3166 alpha-2. Пример: RU |
| 1 2 | SigningDate | Дата подписания | + | Nullable<DateTime> | |
| 1 3 | ValidFrom | Дата начала действия сертификата | + | DateTime | |
| 1 4 | ValidTo | Дата окончания действия сертификата. | + | DateTime | |
| 1 5 | CertificateValidationSource | Источник проверки сертификата на валидность | - | CertificateValidationSource | |

14. Тип: DetachedSignatureEx

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения /Тип | Комментарий |
|---|-------------------------|----------------------------------|----------------|------------------------|-------------|
| 1 | Body | Содержимое отсоединенной подписи | + | Byte[] | |
| 2 | DetachedSignatureFormat | Тип отсоединенной подписи | - | CMS, CAESBES, CAESX | |

15. Тип: DetachedSignature

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения /Тип | Комментарий |
|---|---------------|----------------------------------|----------------|------------------------|-------------|
| 1 | Body | Содержимое отсоединенной подписи | + | Byte[] | |
| 2 | MimeType | МIME-тип данных подписи | - | String | |

16. Тип: ImageBase64

| № | Код параметра | Описание параметра | Обязательность | Способ заполнения /Тип | Комментарий |
|---|----------------|---|----------------|------------------------|-------------|
| 1 | Base64 | Содержимое изображения страницы документа | + | String | |
| 2 | ExistNextImage | Признак наличия следующего по счету изображения | + | Boolean | |

17. Перечисление: HashAlgorithmType

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|-----------------------------|
| 1 | SHA1 | 0 | Int32 | Не используется |
| 2 | GOST3411 | 1 | Int32 | ГОСТ Р 34.11 2001 |
| 3 | GOST3411_2012 | 2 | Int32 | ГОСТ Р 34.11 2012 |
| 4 | GOST3411_2012_STRONG | 3 | Int32 | ГОСТ Р 34.11 2012 усиленный |

18. **Перечисление: ClientSignatureFormat**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|-------------|
| 1 | CMS | 1 | Int32 | |
| 2 | CAdESBES | 2 | Int32 | |
| 3 | CAdESX | 3 | Int32 | |
| 4 | XMLDSign | 4 | Int32 | |
| 5 | PAdES | 5 | Int32 | |

19. **Перечисление: SignatureKind**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|------------------------|
| 1 | Attached | 1 | Int32 | Присоединенная подпись |
| 2 | Detached | 2 | Int32 | Отсоединенная подпись |

20. **Перечисление: ClientSigningMode**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|--|
| 1 | Separately | 1 | Int32 | Подписание каждого файла отдельно с выбором своей ЭП |
| 2 | Batch | 2 | Int32 | Подписание всех файлов однократно выбранной ЭП |

21. **Перечисление: OperationType**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|--------------------------|-------------------|---------------------------|---|
| 1 | CreateUIToSign | 1 | Int32 | Создание интерфейса для просмотра и подписания документов |
| 2 | CreateUIToShowSignatures | 2 | Int32 | Создание интерфейса для просмотра информации о |

| | | | | |
|---|-------------------------|---|-------|--|
| | | | | подписях |
| 3 | CreateUIToShowDocuments | 3 | Int32 | Создание интерфейса для просмотра документов |

22. **Перечисление: OperationState**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|------------------------------------|
| 1 | Initial | 1 | Int32 | Новая операция |
| 2 | Processed | 2 | Int32 | Операция выполняется |
| 3 | NotFound | 3 | Int32 | Зарезервировано |
| 4 | Expired | 4 | Int32 | Время доступности операции истекло |
| 5 | Error | 5 | Int32 | Ошибка выполнения |

23. **Перечисление: ServerSignatureFormat**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|-------------|
| 1 | CMS | 1 | Int32 | |

24. **Перечисление: CertificateValidationSource**

| № | Наименование элемента | Значение элемента | Способ заполнения/ Тип | Комментарий |
|---|-----------------------|-------------------|---------------------------|---------------------|
| 1 | External | 0 | Int32 | Внешний сервис |
| 2 | Internal | 1 | Int32 | Внутренняя проверка |