



КриптоАРМ АРІ

Оглавление

Описание API КриптоАРМ	2
1. Команда sign. Запрос на подпись документов	3
1.1. Формат ссылки.....	4
1.2. Формат JSON	4
1.2.1. Интерфейс IParameters.....	4
1.2.2. Интерфейс IFile.....	4
1.2.3. Интерфейс IExtra	5
1.2.4. Пример	5
1.3. Интерфейс КриптоАРМ при подписи документов.....	6
2. Команда verify. Запрос на проверка подписи.....	7
2.1. Формат ссылки.....	8
2.2. Формат JSON	8
2.2.1. Интерфейс IParameters.....	8
2.2.2. Интерфейс IFile.....	8
2.2.3. Интерфейс IExtra	8
2.2.4. Пример	9
2.3. Интерфейс КриптоАРМ при проверке подписи.....	9

Описание API КriptoAPM

Доступно множество команд, которые взаимодействуют с КriptoAPM. Все они открывают КriptoAPM, если он не запущен. Их можно ввести через адресную строку браузера (вы можете размещать их так же, как ссылки на веб-страницы) или в терминале (для Windows интерпретатор команд). Для взаимодействия используется зарегистрированный протокол **cryptoarm://**

В текущей редакции доступны команды:

- **sign** – запрос на электронную подпись документа или пакета документов
- **verify** – запрос на проверку электронной подписи документа или пакета документов

Общий сценарий выполнения команд (для взаимодействия с web-приложениями):

1. Пользователь заходит на портал (web-приложение).
2. Выбирает объекты (например список документов) и действие (например подпись).
3. Портал генерирует и отображает (или сразу переходит) ссылку с протоколом **cryptoarm://**
4. Если КriptoAPM не запущен, то запускается. Затем обращается к portalу за JSON с набором параметров, нужных для выполнения конкретной операции. JSON генерируется на сервере, где располагается web-приложение.
5. Полученный JSON обрабатывается и в зависимости от команды выполняются нужные дополнительные запросы к web-приложению.
6. Пользователь выполняет саму запрошенную операцию (остальной функционал приложения блокируется).
7. Результаты отправляются на сервер.

Общий формат ссылки:

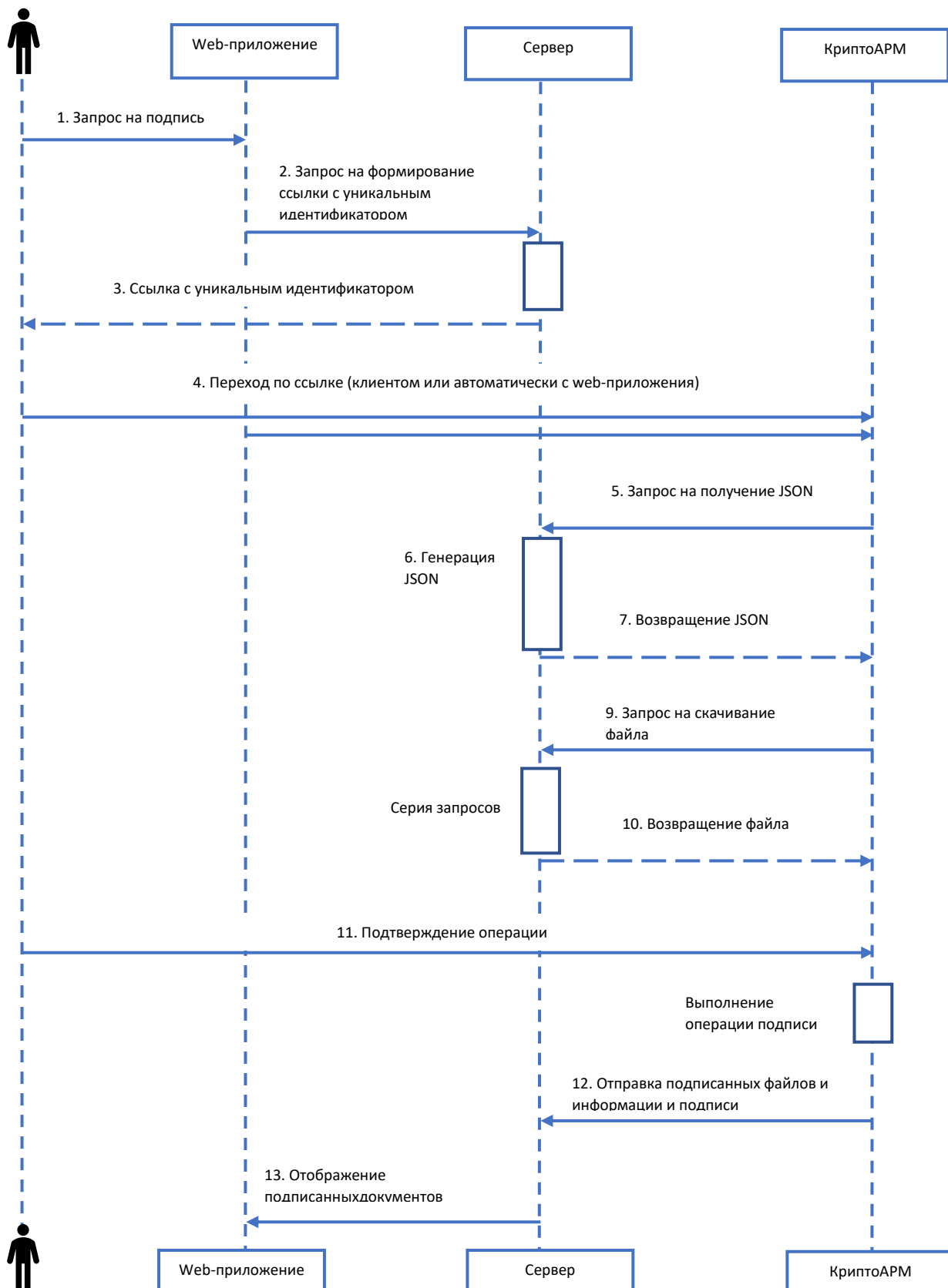
cryptoarm://<command> /<URL>/[?key1=parameter1&key2=parameter2...]

Здесь:

- **cryptoarm://** - зарегистрированный протокол
- **<command>** - выполняемая команда
- **<URL>** - ссылка на получение JSON с параметрами, нужными для выполнения команды
- **[?key1=parameter1&key2=parameter2...]** - дополнительные параметры (необязательные и могут отличаться для разных команд).

1. Команда sign. Запрос на подпись документов

Команда **sign** (подпись) используется для запроса на подпись документа или пакета документов. Выполнение операции требует действующей лицензии на КристоАРМ ГОСТ. Схема взаимодействия:



1.1. Формат ссылки

Для выполнения подписи документов должна быть сформирована ссылка вида:

cryptoarm://sign/<URL>/[?key1=parameter1&key2=parameter2...]

Здесь:

- **cryptoarm://** - зарегистрированный протокол
- **sign** - выполняемая команда
- **<URL>** - ссылка на получение JSON с параметрами, нужными для выполнения команды
- **[?key1=parameter1&key2=parameter2...]** - дополнительные параметры (необязательные и могут отличаться для разных команд). Пример параметра: `accessToken`, который используется для получения JSON с параметрами операций.

Пример:

`cryptoarm://sign/https://example.com/json?accessToken=2c48eb32-a0a8-405c-ade9-eed130605cba`

1.2. Формат JSON

После получения команды **sign** КристоАРМ отправляет запрос на получение JSON с параметрами операции. Формат JSON:

Ключ	Значение	Описание
method	sign	Используемый метод или вид команды
params	Объект типа IParameters	Параметры выполнения команды

1.2.1. Интерфейс IParameters

Интерфейс IParameters описывает параметры операции.

Свойство	Тип	Описание
license ?	string	Необязательное свойство. Содержит временную лицензию, которая будет использоваться для выполнения операции в КристоАРМ
uploader	string	Ссылка, на которую будут отправлены подписанные файлы
files	Массив типа IFile[]	Массив файлов на подпись
extra	Объект типа IExtra	Настройки операции

1.2.2. Интерфейс IFile

Интерфейс IFile описывает файлы и ссылки на них.

Свойство	Тип	Описание
name	string	Имя файла (с расширением)
url	string	Ссылка на скачивание файла
id	string	Уникальный идентификатор файла
urlDetached ?	string	Необязательный параметр. Используется для откреплённой подписи

1.2.3. Интерфейс IExtra

Интерфейс IExtra описывает настройки операции.

Свойство	Тип	Описание
signType	string	Необязательный параметр. Возможные значения: 0 - присоединенная подпись 1 - отсоединённая подпись
signStandart	string	Необязательный параметр. Стандарт подписи. Возможные значения: 0 - CMS 1 - CaDES-X Long Type1
token	string	Необязательный параметр. Токен, который будет использоваться при скачивании файлов с сервиса (параметр запроса)

1.2.4. Пример

```
{
  "method": "sign",
  "params": {
    "license": "",
    "token": "",
    "files": [
      {
        "name": "file1.txt",
        "url": "http://localhost:8080/public/files/file1.txt",
        "id": 1,
        "urlSign": ""
      },
      {
        "name": "file2.txt",
        "url": "http://localhost:8080/public/files/file2.txt",
        "id": 2,
        "urlSign": ""
      },
      {
        "name": "file4.pdf",
        "url": "http://localhost:8080/public/files/file4.pdf",
        "id": 4,
        "urlSign": ""
      }
    ],
    "extra": {
      "token": "9c7101f7-9c47-4481-b4da-a6a497abde08",
      "signType": "1",
      "signStandart": "1"
    }
  }
}
```

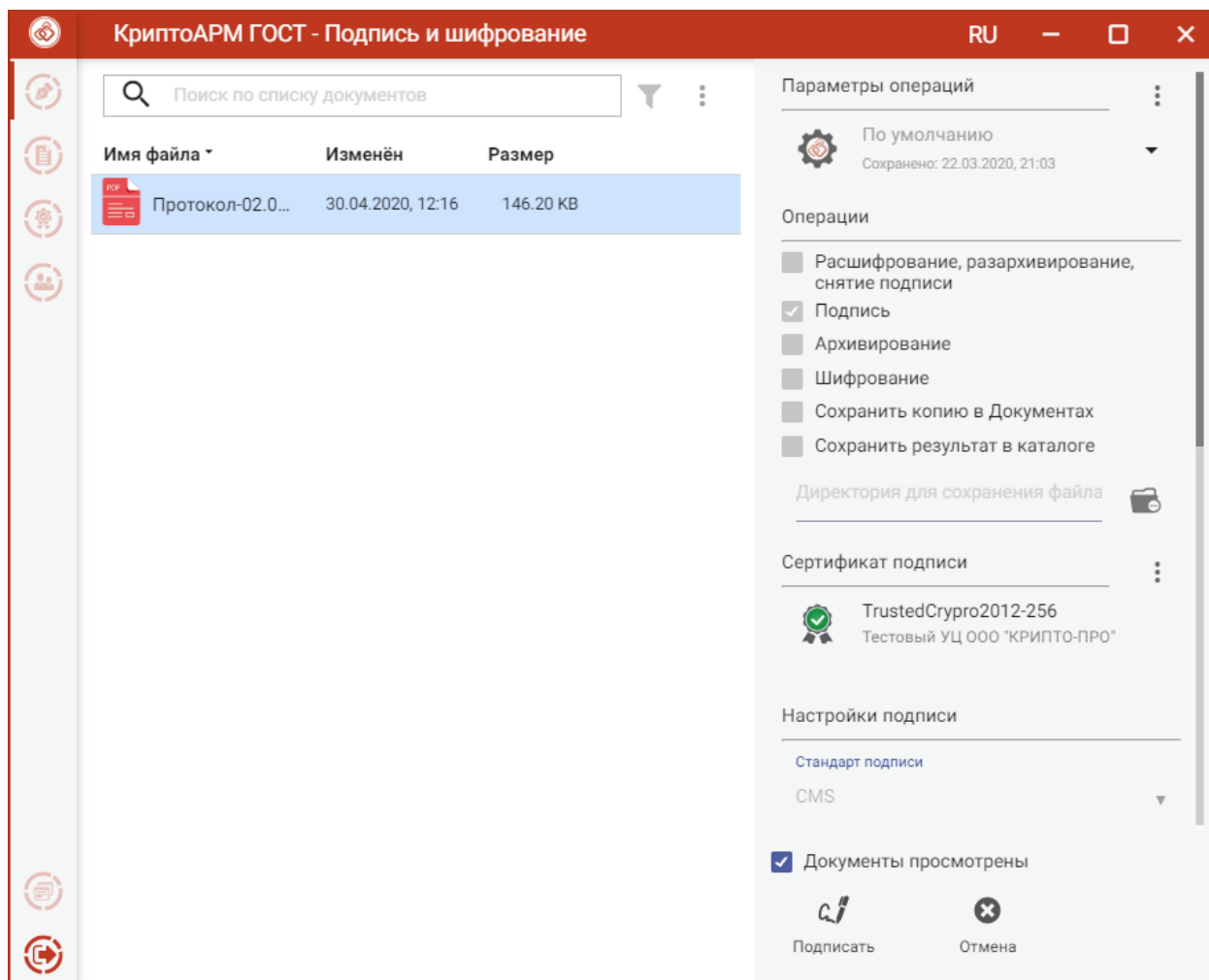
```

    },
    "uploader": "http://localhost:8080/upload"
  }
}

```

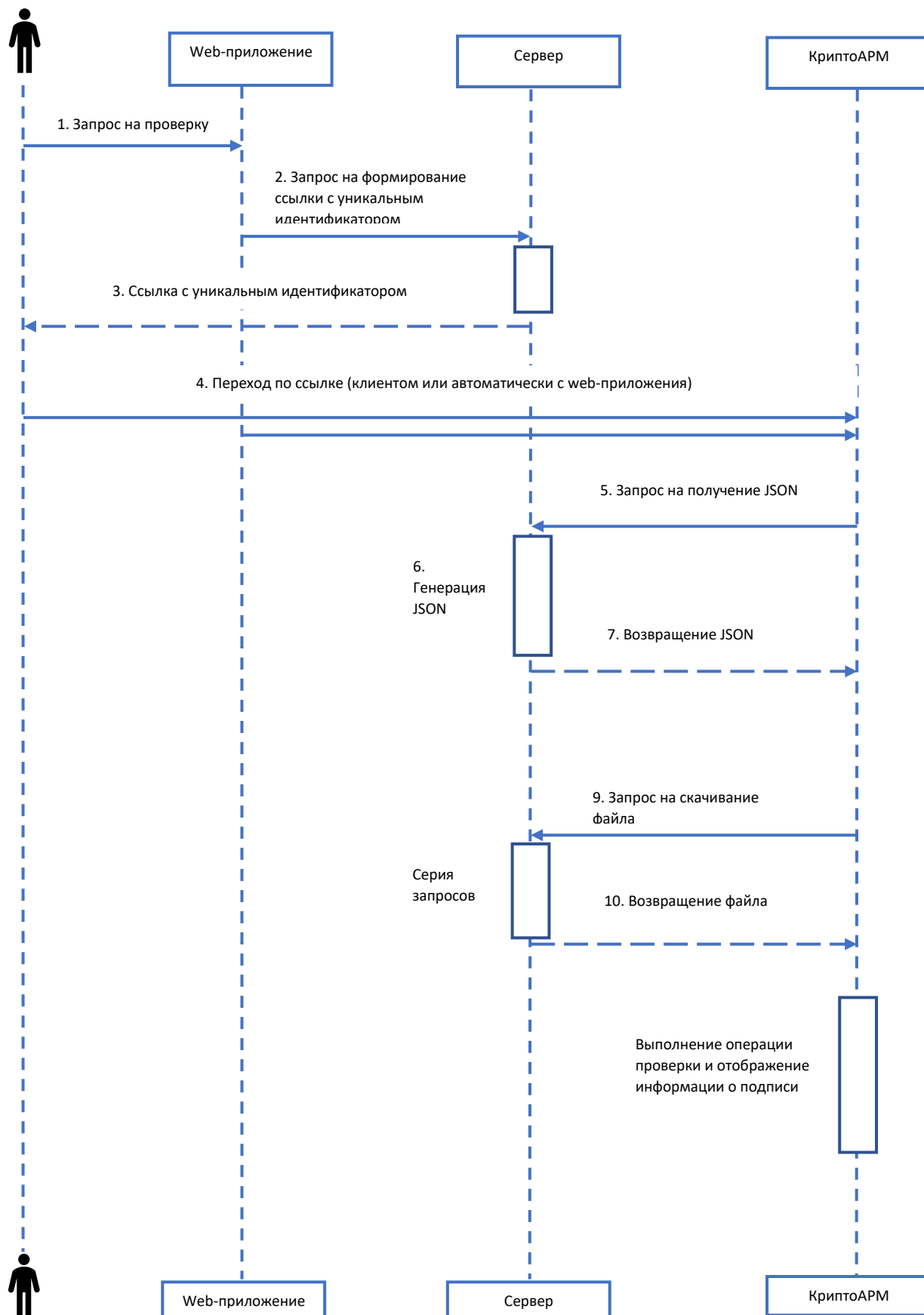
1.3. Интерфейс КриптоАРМ при подписи документов

При выполнении операции подписи по ссылке, не относящийся к процедуре интерфейс блокируется. Пользователю доступны: выбор сертификата, часть настроек подписи. Кнопка «Выполнить» заменяется двумя: «Подпись» и «Отмена». После выполнения команды, приложение будет свернуто в системный трей.



2. Команда verify. Запрос на проверка подписи

Команда **verify** (проверка) используется для запроса на проверку подписи документа или пакета документов. Схема взаимодействия:



2.1. Формат ссылки

Для выполнения подписи документов должна быть сформирована ссылка вида:

cryptoarm://verify/<URL>/[?key1=parameter1&key2=parameter2...]

Здесь:

- **cryptoarm://** - зарегистрированный протокол
- **verify** - выполняемая команда
- **<URL>** - ссылка на получение JSON с параметрами, нужными для выполнения команды
- **[?key1=parameter1&key2=parameter2...]** - дополнительные параметры (необязательные и могут отличаться для разных команд). Пример параметра: `accessToken`, который используется для получения JSON с параметрами операций.

Пример:

`cryptoarm://verify/https://example.com/json?accessToken=2c48eb32-a0a8-405c-ade9-eed130605cba`

2.2. Формат JSON

После получения команды **verify** КриптоАРМ отправляет запрос на получение JSON с параметрами операции. Формат JSON:

Ключ	Значение	Описание
method	verify	Используемый метод или вид команды
params	Объект типа IParameters	Параметры выполнения команды

2.2.1. Интерфейс IParameters

Интерфейс IParameters описывает параметры операции.

Свойство	Тип	Описание
files	Массив типа IFile[]	Массив файлов на подпись
extra	Объект типа IExtra	Настройки операции

2.2.2. Интерфейс IFile

Интерфейс IFile описывает файлы и ссылки на них.

Свойство	Тип	Описание
name	string	Имя файла (с расширением)
url	string	Ссылка на скачивание файла
id	string	Уникальный идентификатор файла
urlDetached ?	string	Необязательный параметр. Используется для откреплённой подписи

2.2.3. Интерфейс IExtra

Интерфейс IExtra описывает настройки операции.

Свойство	Тип	Описание
token	string	Необязательный параметр. Токен, который будет использоваться при скачивании файлов с сервиса (параметр запроса)

2.2.4. Пример

```
{
  "method": "verify",
  "params": {
    "files": [
      {
        "name": "file1.txt",
        "url": "http://localhost:8080/public/files/file1.txt",
        "id": 1,
        "urlSign": ""
      },
      {
        "name": "file2.txt",
        "url": "http://localhost:8080/public/files/file2.txt",
        "id": 2,
        "urlSign": ""
      },
      {
        "name": "file4.pdf",
        "url": "http://localhost:8080/public/files/file4.pdf",
        "id": 4,
        "urlSign": ""
      }
    ],
    "extra": {
      "token": "9c7101f7-9c47-4481-b4da-a6a497abde08",
    },
  },
}
```


2.3. Интерфейс КриптоАРМ при проверке подписи

При выполнении операции проверки по ссылке, не относящийся к процедуре интерфейс блокируется. Пользователю доступны: выбор сертификата, часть настроек подписи. Кнопка «Выполнить» заменяется двумя: «Проверить» и «Отмена». После выполнения команды, приложение будет свернуто в системный трей.


КриптоАРМ ГОСТ - Подпись и шифрование

RU

Поиск по списку документов


Имя файла	Изменён	Размер
 1.png.sig	30.04.2020, 12:19	91.82 KB

Информация о подписи



Подпись действительна

Проверена: 30.04.2020, 12:19



1.png.sig

30.04.2020, 12:19 91.82 KB

Свойства подписи:

Стандарт подписи: CMS

Подписано: 30 апреля 2020 г., 11:12

Сертификат подписчика:

Антонов Антон Антонович

Владелец сертификата

Тестовый УЦ ООО "КРИПТО-ПРО"

Кем выдан

10 июня 2020 г., 15:04

Годен до

ГОСТ Р 34.11-2012/34.10-2012 256 бит


Алгоритм подписи

Цепочка сертификации

2

Тестовый УЦ ООО "КРИПТО-ПРО"


Тестовый УЦ ООО "КРИПТО-ПРО"



1

Антонов Антон Антонович

Тестовый УЦ ООО "КРИПТО-ПРО"



< НАЗАД