КОД безопасности

Программа доверенной визуализации и подписи

Jinn-Client

Версия 2

Руководство администратора

RU.АМБС.58.29.12.010 91

Почтовый адрес:	**115127, Россия, Москва, а/я 66 ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

КЦ	Контроль целостности
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

Введение

Данное руководство предназначено для администраторов изделия "Программа доверенной визуализации и подписи Jinn-Client. Версия 2" RU.АМБС.58.29.12.010 (далее — Jinn-Client, изделие). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации Jinn-Client.

Сайт в интернете. Информация о продуктах компании "Код Безопасности" представлена на сайте https://www.securitycode.ru.

Служба технической поддержки. Связаться со службой технической поддержки можно по телефону 8 800 505-30-20 или по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Список учебных центров и условия обучения представлены на сайте компании https://www.securitycode.ru/company/education/training-courses/.

Глава 1
Общие сведения

Назначение и основные функции Jinn-Client

Jinn-Client предназначен для формирования ЭП электронного документа, расположенного в оперативной памяти компьютера в виде XML-документа, текстового или бинарного файла. Формирование ЭП осуществляется в соответствии с положениями ст. 12 Федерального закона РФ "Об электронной подписи" от 06.04.2011 №63-ФЗ.

Jinn-Client реализует следующие основные функции:

- формирование ЭП в соответствии с криптографическим алгоритмом ГОСТ Р 34.10–2012 с функцией хэширования по ГОСТ Р 34.11–2012;
- формирование ЭП в форматах XMLDSig, XAdES-BES, CMS, CAdES-BES;
- формирование ЭП в среде операционной системы семейства Linux в графическом режиме;
- формирование ЭП серии документов — одна подпись под каждым документом;
- проверка корректности сформированной ЭП;
- доверенная визуализация документов в форматах txt, xml, pdf, bin средствами Jinn-Client;
- генерация ключей ЭП в криптографических контейнерах формата PKCS#15 и формирование запросов формата PKCS#10 на выпуск сертификатов ключей проверки ЭП в соответствии с методическими рекомендациями ТК 26;
- чтение ключей, сгенерированных средством криптографической защиты информации "КриптоПро CSP" версий 4, 5;
- фильтрация ключей для формирования ЭП;
- контроль целостности установленного ПО Jinn-Client.

Состав Jinn-Client

Jinn-Client состоит из следующих программных компонентов, объединенных под единым интерфейсом управления:

- модуль генерации ключей ЭП;
- модуль визуализации;
- модуль формирования ЭП;
- модуль взаимодействия с ключевыми носителями;
- модуль интерфейсов взаимодействия (API).

Варианты исполнения

Jinn-Client может функционировать совместно с изделием "Программно-аппаратный комплекс "Соболь" версий 3.0/3.1/3.2 (далее — ПАК "Соболь").

Jinn-Client выпускается в следующих вариантах исполнения.

№ исп.	Наименование исполнения	Применение ПАК "Соболь"	Формирование и проверка ЭП	Вычисление хэш-функции
1	Программа доверенной визуализации и подписи Jinn-Client. Версия 2	Нет	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012
2	Программа доверенной визуализации и подписи Jinn-Client. Версия 2	Да	ГОСТ Р 34.10–2012	ГОСТ Р 34.11–2012

Jinn-Client в исполнении 1 соответствует требованиям ФСБ России к криптографическим средствам класса КС1, а в исполнении 2 — класса КС2.

Внимание! Отсутствие на компьютере ПАК "Соболь" для исполнения 2 блокирует работу программного обеспечения Jinn-Client.

Принципы функционирования

Ключевые носители

Персональный ключевой носитель, выдаваемый пользователю администратором, предназначен для хранения ключевой информации — ключа ЭП и сертификата ключа проверки ЭП. Ключ ЭП однозначно соответствует сертификату ключа проверки ЭП. При подписании документа пользователь предъявляет ключевой носитель, ключевая информация считывается с носителя и с ее помощью создается ЭП.

Для предотвращения несанкционированного использования ключа ЭП посторонними лицами ключ защищают паролем.

В качестве ключевых носителей при работе с Jinn-Client могут использоваться USB-флеш-накопители и электронные идентификаторы (смарт-карты и USB-токены).

Поддерживается работа со следующими ключевыми носителями:

Устройство	**Примечание**
Смарт-карты	
Рутокен ЭЦП 2.0	Не поддерживается работа с ключами Jinn-Client 1* и ключами КриптоПро CSP**
Рутокен ЭЦП (PKI)	Не поддерживается работа с ключами Jinn-Client 1* и ключами КриптоПро CSP**
Рутокен Lite	Не поддерживается работа с ключами Jinn-Client 1* и ключами КриптоПро CSP**
JaCarta PKI	
JaCarta ГОСТ	
JaCarta-2 ГОСТ	Не поддерживается работа с ключами КриптоПро CSP**
USB-токены	
Рутокен S	Не поддерживается запись ключа на устройство
Рутокен ЭЦП 2.0	
Рутокен Lite	
JaCarta PKI	
JaCarta ГОСТ	
JaCarta LT	Не поддерживается работа с ключами КриптоПро CSP**
ESMART Token GOST	Не поддерживается работа с ключами КриптоПро CSP**
ESMART Token 64k	Ограниченная поддержка. Требуется инициализация в особом режиме. Рекомендуется обратиться в службу технической поддержки ООО "Код Безопасности"
JaCarta-2 ГОСТ	Не поддерживается работа с ключами КриптоПро CSP**

* Ключ Jinn-Client 1 — ключ, сгенерированный средствами изделия "Программно-аппаратный комплекс квалифицированной электронной подписи "Jinn" / Программа доверенной визуализации и подписи "Jinn-Client" версии 1.0".
** Ключ КриптоПро CSP — ключ, сгенерированный средствами изделия "Средство криптографической защиты информации "КриптоПро CSP".

Для доступа к памяти USB-токена или смарт-карты необходимо ввести специальный пароль — PIN-код. По умолчанию идентификатор защищен стандартным PIN-кодом, который задается производителем. Если стандартный PIN-код не был изменен, Jinn-Client автоматически осуществляет доступ к памяти идентификатора при его предъявлении. В том случае, если стандартный PIN-код был изменен, пользователь при каждом предъявлении идентификатора должен вводить значение PIN-кода в соответствующем окне диалогового интерфейса.

Дополнительно для входа в ПАК "Соболь" пользователю изделия может потребоваться:

- идентификатор iButton (DS1992, DS1993, DS1994, DS1995, DS1996);
- USB-токен (eToken PRO, eToken PRO Java, iKey 2032, Rutoken, Rutoken RF);
- смарт-карта eToken PRO.

Доверенная визуализация

Jinn- Client обеспечивает визуальное представление содержимого подписываемого документа непосредственно перед подписанием для подтверждения пользователем операции по формированию ЭП. Визуализация позволяет выявить подмену содержимого документа перед подписанием и отказаться от подписи подложного документа.

Jinn-Client поддерживает следующие режимы визуализации документов:

- все документы;
- выбранные документы;
- без визуализации.

Доверенная визуализация документов в форматах txt, xml, pdf, bin осуществляется средствами ПО Jinn-Client.

Просмотр документов при подписании может осуществляться средствами стороннего ПО, но в этом случае визуализация не будет считаться доверенной.

Контроль целостности установленного ПО

Функция контроля целостности предназначена для слежения за неизменностью содержимого установленного ПО. Контролю подлежат все служебные файлы ПО Jinn-Client, размещенные в каталоге установки и системных папках ОС.

Действие функции КЦ основано на проверке электронной подписи контролируемых файлов, сформированной во время сборки релиза ПО предприятием-изготовителем.

Проверка электронной подписи контролируемых файлов выполняется в следующих случаях:

- автоматически после установки ПО Jinn-Client;
- автоматически раз в сутки;
- при запуске Jinn-Client, если проверка не выполнялась в течение последних суток;
- вручную по команде администратора.

При отрицательном результате проверки КЦ на экран выводится соответствующее сообщение. Для дальнейшего продолжения работы администратору необходимо переустановить ПО Jinn-Client.

Запуск процедуры проверки электронной подписи контролируемых файлов вручную описан в Приложении (см. стр.**27**).

Контроль целостности в исполнении 2

Контроль целостности в исполнении 2 осуществляется средствами ПАК "Соболь". В этом варианте исполнения процедура контроля целостности выполняется при каждом запуске ОС.

Для настройки контроля целостности необходимо выполнить следующее:

1. Загрузить в компьютер шаблон контроля целостности, входящий в состав ПО Jinn-Client.
2. В настройках ПАК "Соболь" указать путь к загруженному шаблону (см. эксплуатационную документацию ПАК "Соболь").
3. В ПАК "Соболь" выполнить расчет эталонных значений котрольных сумм (см. эксплуатационную документацию ПАК "Соболь").

Лицензирование

ПО Jinn-Client поставляется со встроенной демо-лицензией. По истечении 14 дней с момента установки Jinn-Client необходимо зарегистрировать лицензию, полученную у предприятия-изготовителя. В отсутствие зарегистрированной лицензии по истечении 14 дней функции Jinn-Client становятся недоступными, за исключением процедуры регистрации лицензии. После регистрации лицензии доступ восстанавливается.

Предусмотрено два типа лицензий: базовая и расширенная. Базовая лицензия предусматривает работу только с ключами формата PKCS#15. Расширенная лицензия позволяет работать как с ключами формата PKCS#15, так и с ключами, сгенерированными СКЗИ "КриптоПро CSP".

Работа с лицензиями описана на стр.**17**.

Системные требования

Компьютеры, на которых предполагается использовать Jinn-Client, должны соответствовать следующим аппаратным и программным требованиям:

Операционная система x64	• Astra Linux Common Edition 2.12 "Орел" (kernel version 4.15.3); • Astra Linux Special Edition 1.5 (kernel version 4.2.0); • Astra Linux Special Edition 1.6 "Смоленск"; • CentOS 7.2 (kernel version 3.10); • RHEL 7.5 Desktop x64 (3.10 kernel version); • Ubuntu 16.04 LTS Desktop (версия ядра linux 4.4); • Ubuntu 18.04 LTS Desktop (версия ядра linux 4.15); • Альт Линукс СПТ 7.0.5 (ядро Linux 3.14); • Альт Линукс 8.2 (ядро Linux 4.9); • РЕД ОС 7.1 МУРОМ (Linux Kernel 4.9); • ROSA Enterprise Desktop (RED) X3 (Linux Kernel 4.9.41)
Операционная система x32	• Альт Линукс 8.2; • CentOS 7.2; • Ubuntu 16.04 LTS Desktop; • ROSA Enterprise Desktop (RED) X3
Процессор (тактовая частота)	Не менее 1,2 ГГц
Оперативная память	Не менее 4 Гбайт
Жесткий диск (свободное место)	Не менее 300 Мбайт
Привод	Привод DVD/CD-ROM

Интерфейсы	2 x USB 2.0; 1 x PCI-E — для исполнения 2; 1 x PCI/PCI-E/Mini PCI-E/Mini PCI-E Half — для исполнения 2
Дополнительное ПО	ПАК "Соболь" — для исполнения 2

Порядок распространения и тиражирования

Установочные модули ПО Jinn-Client и комплект эксплуатационной документации могут поставляться пользователю компанией "Код Безопасности" двумя способами:

- на носителе (CD-, DVD-диски);
- посредством загрузки через интернет.

Для получения возможности загрузки установочных модулей ПО Jinn-Client и комплекта эксплуатационной документации пользователь направляет свои учетные данные Уполномоченной организации. Учетные данные могут быть направлены посредством заполнения специализированной регистрационной формы на сайте Уполномоченной организации.

Установка ПО Jinn-Client на рабочее место пользователя может быть осуществлена только в случае подтверждения целостности полученных установочных модулей ПО Jinn-Client и эксплуатационной документации.

Глава 2
Установка и удаление Jinn-Client

Общий порядок установки Jinn-Client

Установка ПО Jinn-Client состоит из следующих этапов:

1. Установка ПО ПАК "Соболь".

   Если в комплект поставки Jinn-Client входит ПАК "Соболь", то перед установкой ПО Jinn-Client необходимо выполнить установку и настройку ПАК "Соболь". Описание установки и настройки приведено в эксплуатационной документации ПАК "Соболь".

2. Установка драйверов и библиотек для работы с электронными идетификторами.

3. Установка ПО Jinn-Client.

   Для установки используется соответствующий установочный пакет JinnClientv2.0.4- 40- develop- 66a6db.deb или JinnClientv2.0.4- 40- develop- 66a6db.rpm в зависимости от типа ОС.

Установка драйверов и библиотек для работы с электронными идентификторами

Если в качестве ключевых носителей используются электронные идентификаторы (USB-токены и смарт-карты), перед началом установки Jinn-Client необходимо установить драйверы этих устройств. Кроме того, для некоторых устройств может потребоваться установка дополнительных пакетов и специальных библиотек в зависимости от используемой операционной системы Linux. Требования к устанавливаемому ПО и инструкции приводятся на сайтах вендоров, поставляющих электронные идентификаторы.

Для работы с токенами в системе должны быть установлены библиотеки libccid, pcsclite1, pcscd, а также драйверы для необходимых интерфейсов токенов (APDU и PKCS11).
После установки драйверов и пакетов необходимо убедиться в работоспособности электронных идентификаторов. В случае необходимости следует обращаться в службу поддержки вендора.

Если драйверы установлены, а токены не определяются, необходимо проверить наличие ссылки для библиотеки libpcsclite.so, и при необходимости прописать ее командой ln -s /usr/lib/x86_64-linux-gnu/libpcsclite.so.1 /usr/lib/libpcsclite.so.

В некоторых случаях для поддержки работы с электронными идентификаторами может потребоваться задать или изменить параметры конфигурационного файла libstorage.ini, входящего в состав устанавливаемого программного обеспечения Jinn-Client.

Конфигурационный файл libstorage.ini определяет порядок работы Jinn-Client с разными типами ключевых носителей и может быть расположен в одной из следующих директорий:

- в жестко привязанной директории /opt/securitycode/jc2/etc/libstorage.ini;
- в домашней директории пользователя /<home>/.jc2/libstorage.ini.

Для изменения параметров конфигурационного файла используется любой текстовый редактор.

Внимание! Если конфигурационный файл libstorage.ini в указанных выше директориях отсутствует, его необходимо создать вручную.

Описание параметров конфигурационного файла и пример самого файла приведены в Приложении.

Установка программного обеспечения

Пользователь, устанавливающий ПО Jinn-Client, должен иметь права суперпользователя.

Для установки можно использовать консольный терминал или графический менеджер установки пакетов.

В процессе установки выполняется автоматическая настройка утилиты cron (планировщика задач).

Все события, связанные с установкой и работой Jinn-Client, регистрируются в системном журнале /var/log/syslog или /var/log/messages.

Для установки Jinn-Client в консольном терминале:

1. Запустите консольный терминал и перейдите в папку, в которой находится установочный пакет.
2. Введите команду установки:
   - Для группы ОС, использующих менеджер пакетов deb, используйте команду **sudo dpkg -i JinnClientv2.0.4-40-develop-66a6db.deb**.
   - Для группы ОС, использующих менеджер пакетов rpm, используйте команду **sudo yum install JinnClientv2.0.4-40-develop-66a6db.rpm**.
   - Для ОС, использующих отличные от dpkg и yum менеджеры пакетов, необходимо ввести аналогичную команду для соответствующего менеджера пакетов на установку с повышением прав до администратора.

   Начнется установка Jinn-Client.

   Дождитесь сообщения об успешном завершении установки.

   В результате в каталоге **opt** будет создана папка **securitycode** с установленным программным обеспечением Jinn-Client.

Для установки Jinn-Client в графическом менеджере установки пакетов:

1. Откройте установочный пакет в менеджере приложений.

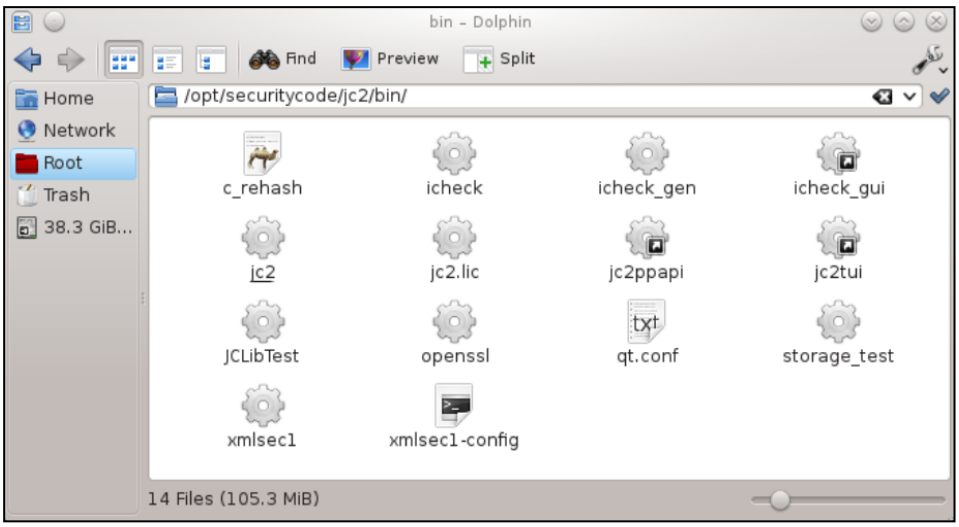
   Откроется окно приложения с информацией о пакете и возможности его установить.
2. Установите пакет, авторизовавшись с правами суперпользователя.

   Jinn-Client будет установлен.

Вызов Jinn-Client

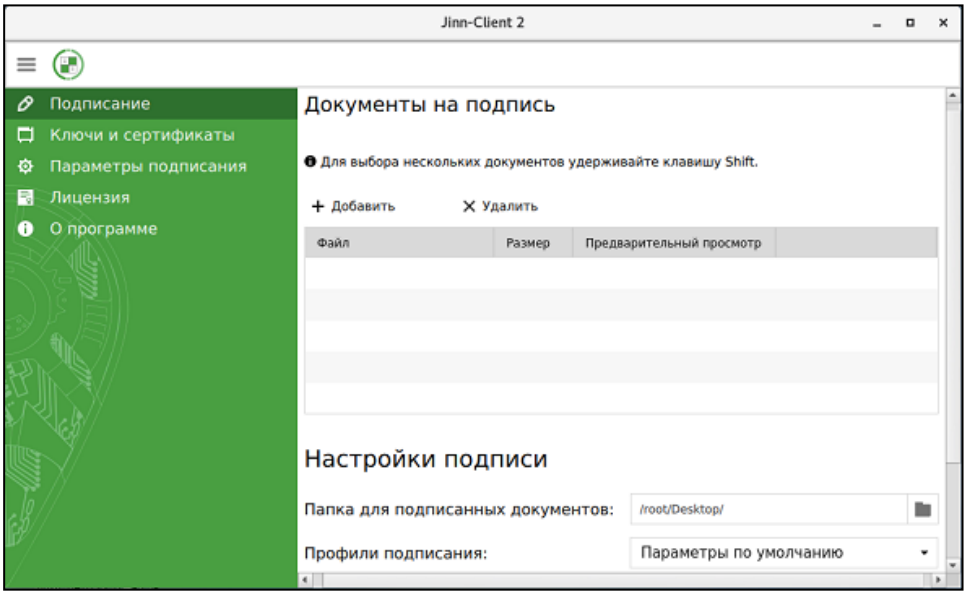
Для вызова Jinn-Client:

1. Перейдите в подкаталог /opt/securitycode/jc2/bin.



2. Запустите исполняемый файл jc2.

   На экране появится главное окно Jinn-Client.

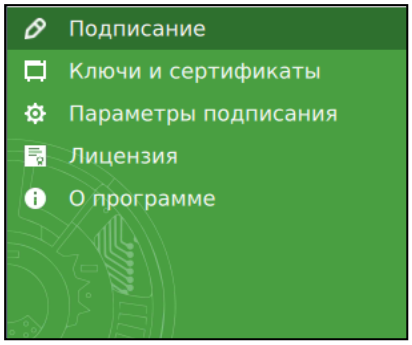


   Описание главного окна приведено в следующем подразделе.

Примечание. Вызвать Jinn-Client можно также можно с помощью ярлыка на рабочем столе или из меню "Пуск".

Главное окно Jinn-Client

В левой части главного окна Jinn-Client расположена панель навигации.



Панель навигации можно минимизировать. Для этого нажмите кнопку , расположенную над панелью.

Для возврата к исходному размеру нажмите кнопку .

Панель навигации состоит из 5 разделов.

Раздел	Описание
Подписание	Подписание документов и настройка процедуры подписания: • задание папки для подписанных документов; • выбор профиля подписания; • включение/отключение предварительного просмотра подписываемого документа; • просмотр содержимого папки с подписанными документами после подписания
Ключи и сертификаты	Работа с ключами: • создание запроса на получение сертификата и формирование ключа; • импорт сертификата и запись на ключевой носитель; • просмотр списка ключей и сертификатов; • копирование ключей на ключевой носитель; • удаление ключей с ключевого носителя
Параметры подписания	Создание, редактирование и удаление профилей подписания. Настройка параметров запроса на выпуск сертификата. Настройка области использования сертификата и политики применения ключа
Лицензия	Загрузка лицензий и просмотр сведений о загруженной лицензии
О программе	Просмотр сведений о версии Jinn-Client

Для выполнения тех или иных действий выберите соответствующий раздел в панели навигации.

Выход из Jinn-Client

Для выхода из Jinn-Client нажмите стандартную кнопку  в правом верхнем углу главного окна.

Удаление Jinn-Client

Пользователь, выполняющий удаление ПО Jinn-Client, должен иметь права суперпользователя.

Удаление Jinn-Client может быть выполнено как в консольном терминале, так и средствами графического пакетного менеджера.

Для удаления в консольном терминале:

- Запустите консольный терминал и введите команду:

  dpkg -r jinnclient2 — для deb

  или

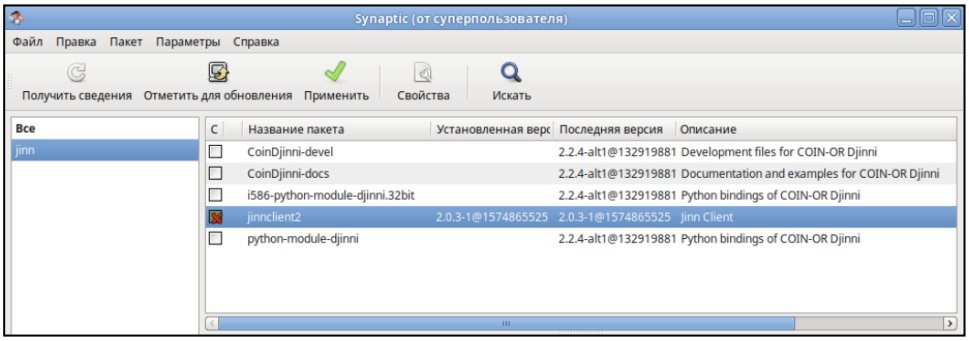
  yum remove jinnclient2 — для rpm.

  Jinn-Client будет удален.

  Для ОС, использующих свой пакетный менеджер, следует запустить аналогичную команду на удаление пакета с правами суперпользователя.

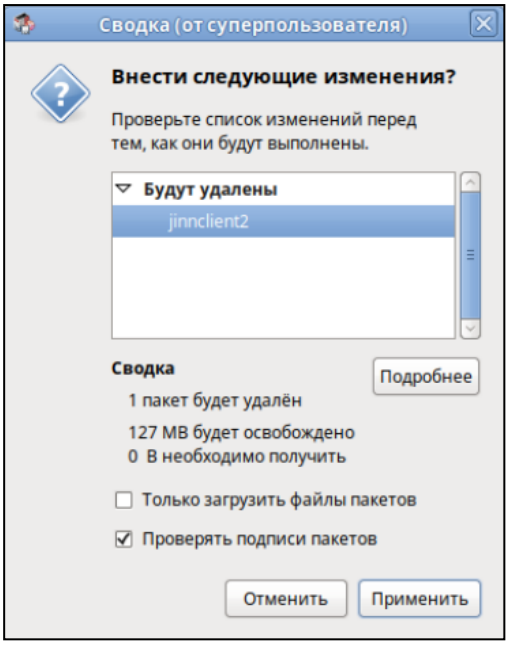
Для удаления в графическом менеджере установки пакетов:

1. Запустите менеджер установки пакетов и выполните поиск всех установленных пакетов.



2. Установите отметку удаления у пакета jinnclient2 и нажмите кнопку "Применить".

   На экране появится окно предупреждения об удалении пакета jinnclient2.



3. Нажмите кнопку "Применить".

   Jinn-Client будет удален.

Обновление

Обновление Jinn- Client выполняется установкой обновленного пакета JinnClientv2.0.4- 40- develop- 66a6db.deb или JinnClientv2.0.4- 40- develop- 66a6db.rpm в зависимости от используемой операционной системы.

Установка выполняется в полном соответствии с описанием установки программного обеспечения (см. стр.**12**).

Глава 3
Подготовка к работе

Общий порядок подготовки Jinn-Client к работе

Подготовка к работе Jinn-Client включает в себя следующие настройки:

1. Регистрация лицензии.
2. Создание профилей подписания.
3. Настройка параметров расширенного запроса на выпуск сертификата.
4. Настройка для работы с веб-порталом.

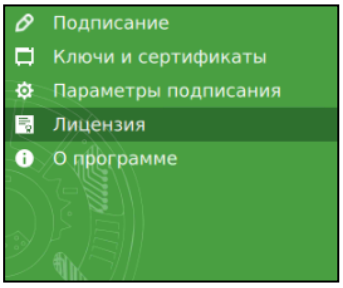
Работа с лицензиями

Лицензия на использование Jinn-Client в виде файла **jc2.lic** входит в состав комплекта поставки программного обеспечения продукта и имеет статус "временная" и тип — базовая.

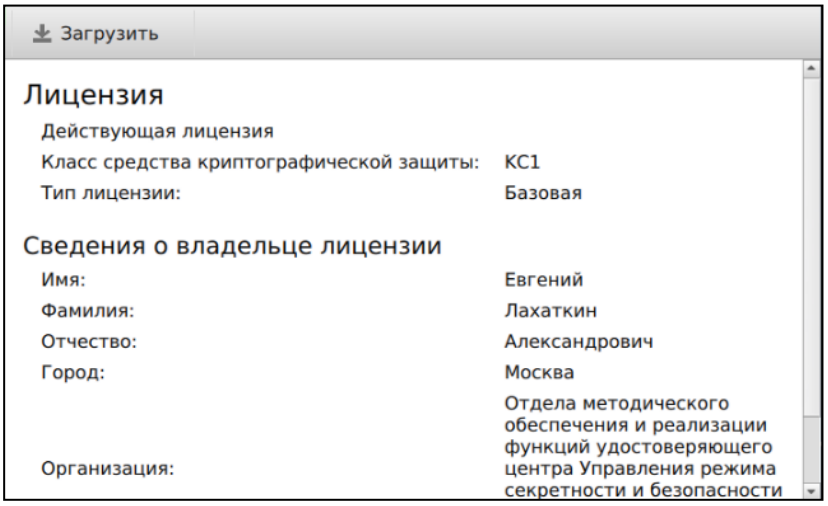
Для продолжения работы по истечении 14 дней с момента установки ПО Jinn-Client необходимо получить и зарегистрировать лицензию со статусом "действующая".

Для просмотра сведений о лицензии:

- В главном окне Jinn-Client выберите раздел "Лицензия".



В окне отобразятся сведения о лицензии.



Сведения о лицензии включают в себя:

- статус — временная, действующая, недействительная;
- класс средства криптографической защиты — КС1 или КС2;
- тип лицензии — базовая или расширенная;
- сведения о владельце лицензии.

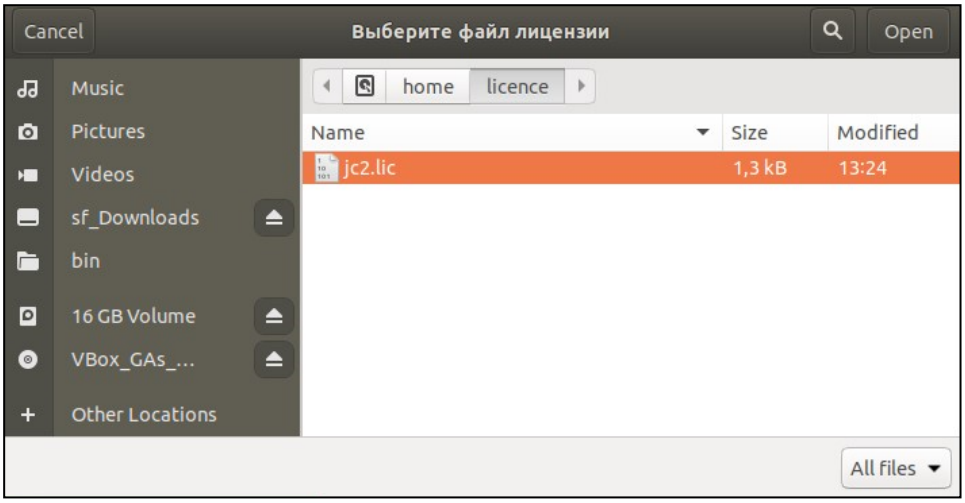
Если регистрация лицензии не выполнялась, в течение 14 дней с момента установки Jinn-Client сведения будут соответствовать временной лицензии.

Если по истечении 14 дней с момента установки Jinn-Client регистрация лицензии не была выполнена, статус лицензии изменится на "недействительная" и работа программы Jinn-Client (за исключением регистрации лицензии) будет заблокирована.

Для регистрации лицензии:

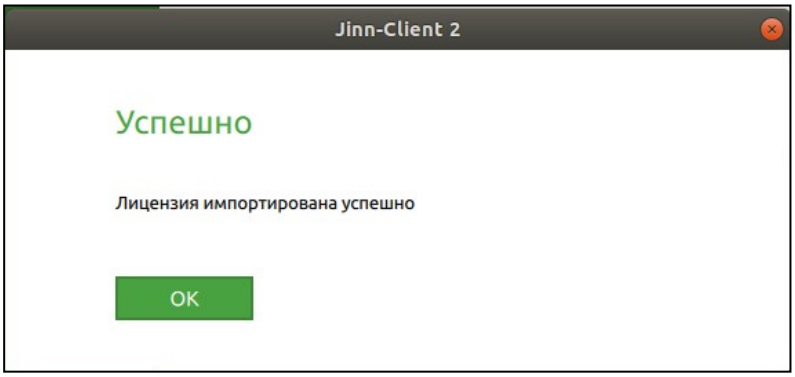
1. Нажмите кнопку "Загрузить".

   На экране появится стандартное окно выбора файла.



2. Откройте папку, в которой хранится файл лицензии, выберите файл и нажмите кнопку "Открыть".

   Будет выполнена проверка лицензии, и в случае положительного результата лицензия будет зарегистрирована. На экране появится сообщение об успешном завершении импорта лицензии.



3. Нажмите кнопку "OK".

Настройка профилей подписания

Профиль подписания — набор параметров электронной подписи, используемый пользователем при подписании документов в Jinn-Client.

Такими параметрами являются:

- Формат — CMS, CAdES-BES, XML или XAdES-BES.
- Присоединенная или отсоединенная подпись.
- Включение или невключение в подпись сертификата ключа подписи.
- Сохранение в формате Base64 или в бинарной кодировке типа DER.

После установки Jinn-Client автоматически создается профиль с параметрами по умолчанию:

- Формат — CMS.

- Присоединенная электронная подпись.
- В подпись включается сертификат владельца.
- Подпись сохраняется в формате Base64.

При необходимости администратор может создать другие профили. Пользователи могут редактировать и удалять профили, созданные администратором.

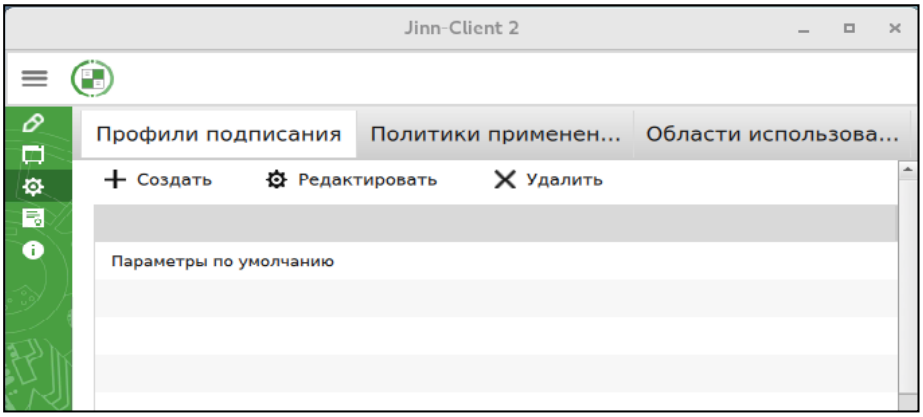
Также предусмотрено копирование созданных профилей для переноса их на другой компьютер или передачи другому пользователю.

Внимание! Профиль с параметрами по умолчанию редактированию и удалению не подлежит.

Для создания нового профиля:

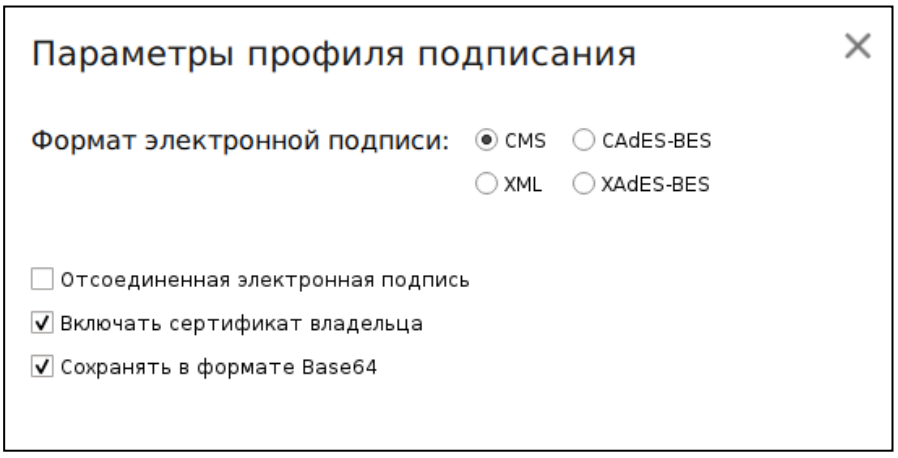
1. В главном окне Jinn-Client выберите раздел "Параметры подписания".

   В окне отобразится список профилей подписания. Если профили не создавались, в списке отобразится только профиль "Параметры по умолчанию".



2. Для просмотра параметров по умолчанию выделите профиль и нажмите кнопку "Редактировать".

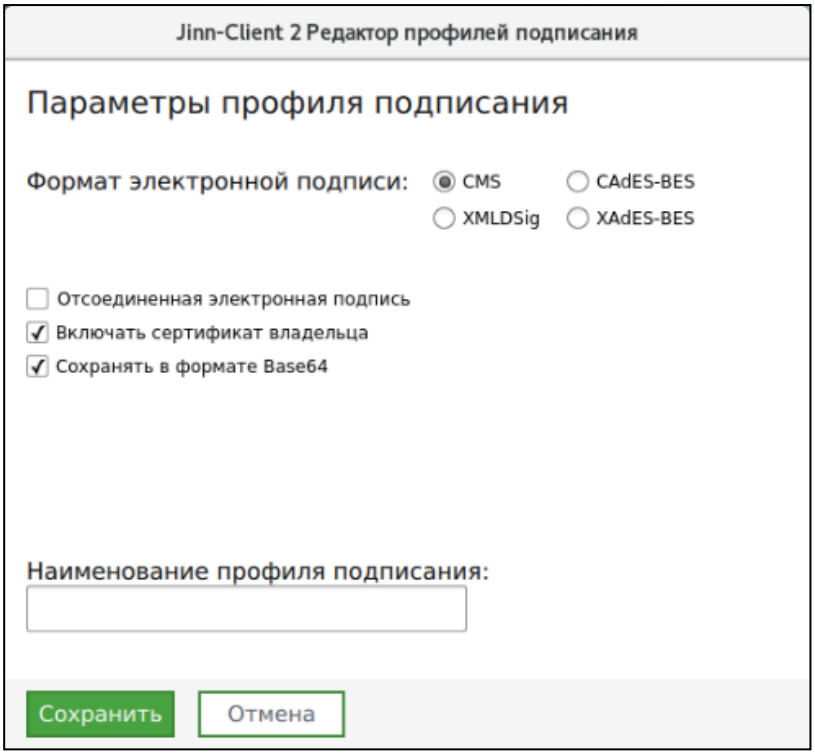
   На экране появится окно с параметрами профиля.



   Внимание! Параметры профиля по умолчанию не редактируются. Поэтому после просмотра закройте окно.

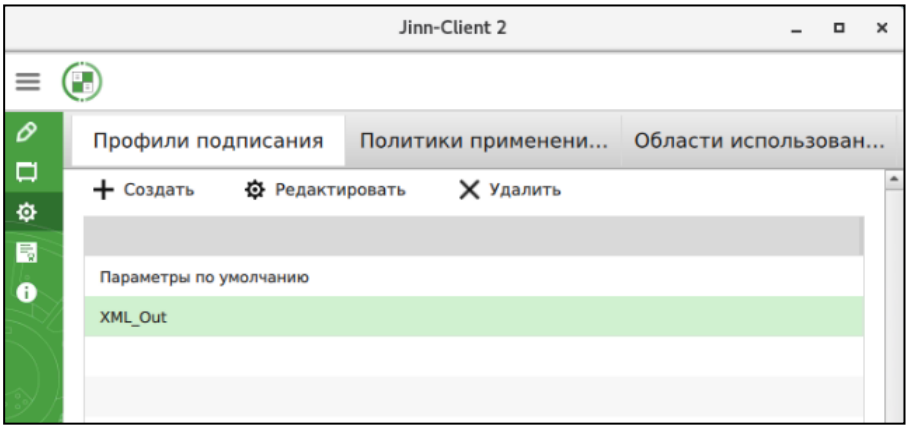
3. В списке профилей нажмите кнопку "Создать".

   На экране появится окно, предназначенное для настройки параметров профиля.



4. Укажите требуемые параметры профиля, введите наименование создаваемого профиля и нажмите кнопку "Сохранить".

   Окно с параметрами профиля закроется, и наименование нового профиля появится в списке.



Профили подписания сохраняются в папке /home/<имя пользователя>/.jc2/JC2SignParameters.

Для редактирования профиля:

1. Выделите профиль в списке и нажмите кнопку "Редактировать".

   Откроется окно с параметрами профиля.

2. Внесите требуемые изменения в параметры профиля и нажмите кнопку "Сохранить".

Для удаления профиля:

- Выделите профиль в списке и нажмите кнопку "Удалить".

  Профиль будет удален.

Для передачи профилей на другой компьютер:

1. Откройте папку /home/<имя пользователя>/.jc2/JC2SignParameters и скопируйте ее содержимое, например, на USB-флеш-накопитель.

2. На другом компьютере с установленным ПО Jinn-Client, на который необходимо установить профили, скопированные в п. **1**, откройте папку /home/<имя пользователя>/.jc2/JC2SignParameters и сохраните в ней все, скопированное в соответствии с п. **1**.

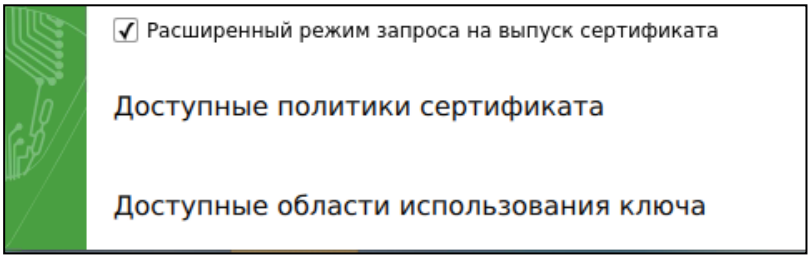
Настройка параметров расширенного запроса на выпуск сертификата

Настройка выполняется в том случае, если сертификаты должны быть получены на основании расширенного режима запроса на выпуск сертификата.

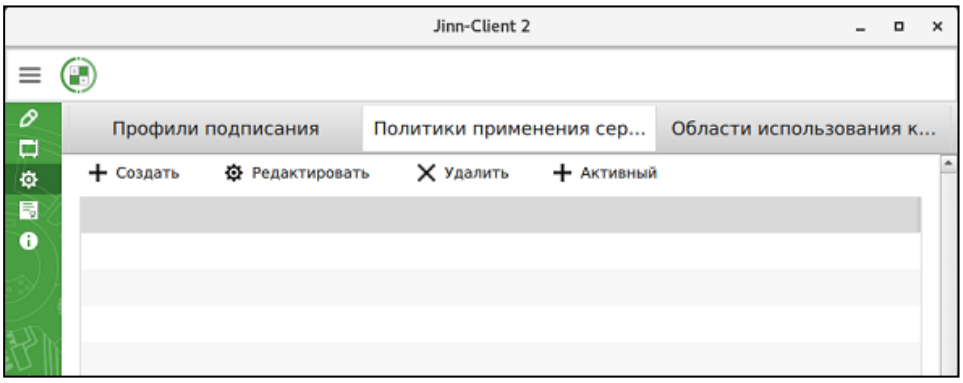
Настройка заключается в задании политик сертификата и областей использования ключа.

Для настройки параметров расширенного запроса:

1. Выберите в панели навигации раздел "Параметры подписания".
2. В нижней части окна установите отметку в поле "Расширенный режим запроса на выпуск сертификата".



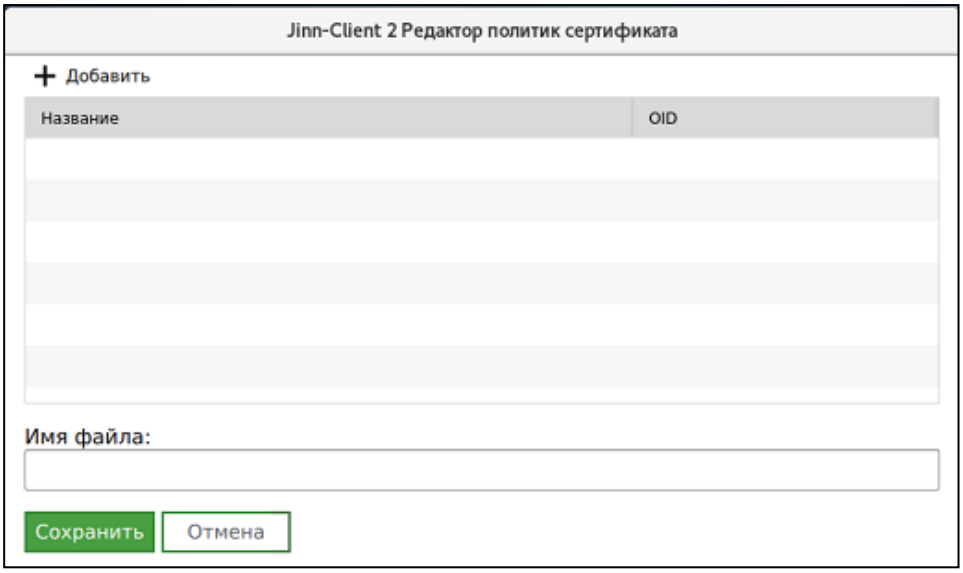
3. Перейдите на вкладку "Политики применения сертификата".



Вкладка предназначена для формирования и редактирования списка политик применения сертификата, которые должны использоваться в запрашиваемом сертификате.

4. Для добавления новой политики в список нажмите кнопку "Создать".

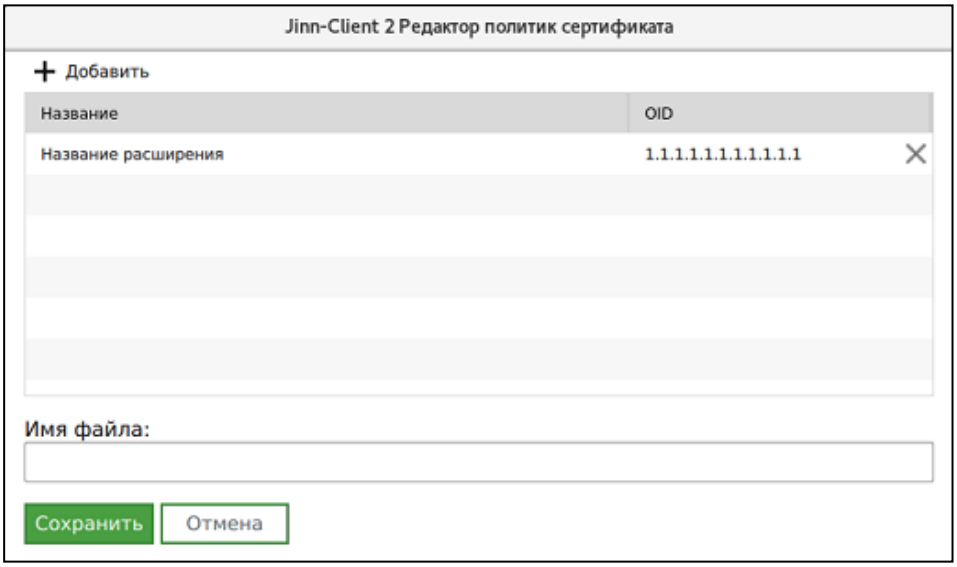
Появится окно "Редактор политик сертификата".



Окно предназначено для формирования и редактирования списка расширений, входящих в состав политики.

5. Для добавления расширения в список нажмите кнопку "Добавить".

   В списке появится шаблон для ввода расширения.



6. Замените в шаблоне название расширения и значение OID.
7. При необходимости добавьте другие расширения в список.

   Для удаления расширения из списка используйте кнопку "X", расположенную справа.
8. После ввода всех необходимых расширений в поле "Имя файла" введите наименование политики и нажмите кнопку "Сохранить".

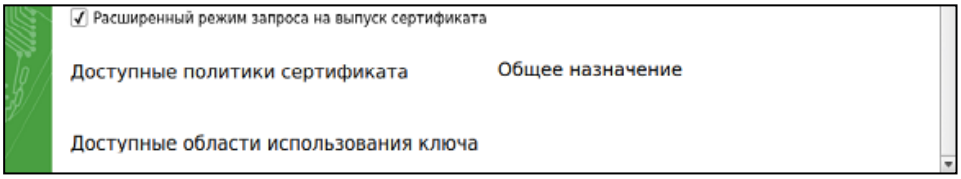
   В списке политик появится новая политика с указанным наименованием.
9. Если для работы предполагается использовать несколько политик, добавьте их в соответствии с описаниями, приведенными в пп. **4**-**8**.

   На рисунке ниже показан список, содержащий 2 политики: "Общее назначение" и "Финансовые операции".

Внимание! Если администратором было создано несколько политик, то пользовтелю, подписывающему документы, будет доступна только одна политика применения сертификата, имеющая статус "активная".

10. Для присвоения статуса политике "активная" выберете в списке политику и нажмите кнопку "+Активная".

    В нижней части окна у параметра "Доступные параметры сертификата" появится наименование выбранной политики (на рисунке ниже — "Общее назначение").



Примечание. Если в дальнейшем потребуется, чтобы активной была другая политика, выберете ее в списке политик и нажмите кнопку "+Активная".

11. Для задания областей использования ключа перейдите на вкладку "Области использования ключа".

    На вкладке появится список областей использования ключа.

Примечание. Если области использования ключа не создавались, список будет пустым.

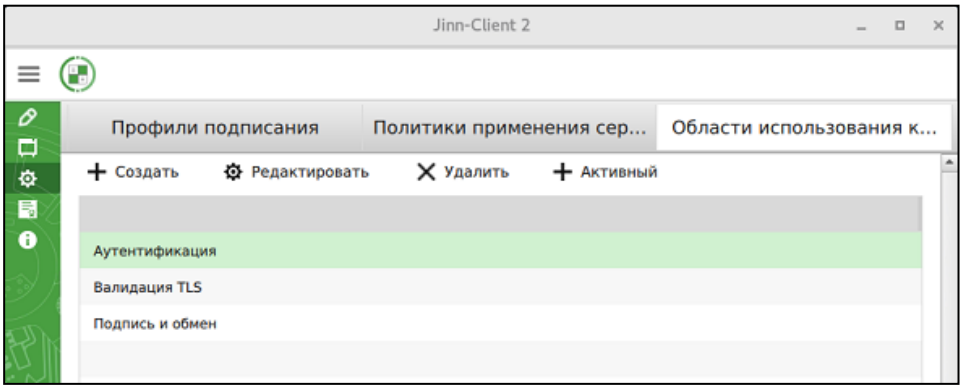
12. Для задания новой области использования ключа нажмите кнопку "+Создать".

    Откроется окно редактора области используемого ключа.

13. Добавьте области используемого ключа в соответствии с описаниями, приведенными в пп. **4**-**8**.

14. Если для работы предполагается использовать несколько областей применения ключа, добавьте их в список.

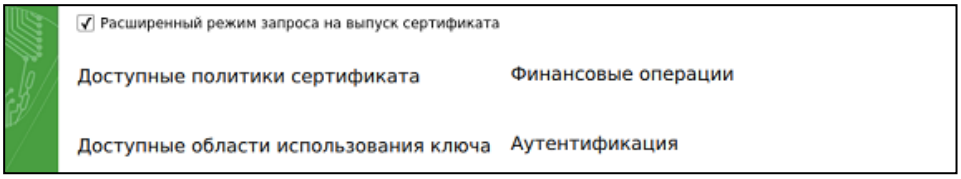
    На рисунке ниже показан список, содержащий 3 области применения ключей.



Внимание! Если администратором было создано несколько областей применения ключа, то пользователю, подписывающему документы, будет доступна только одна область, имеющая статус "активная".

15. Для присвоения статуса области "активная" выберете в списке область и нажмите кнопку "+Активная".

    В нижней части окна у параметра "Доступные области использования ключа" появится наименование выбранной области.



Внимание! Параметры расширенного запроса сохраняются в папке /home/<имя пользователя>/.jc2/JC2ExtensionParameters.

Запись сертификата на ключевой носитель

После получения из УЦ сертификата, выпущенного на основании запроса, сертификат необходимо записать на ключевой носитель, на котором хранится ключ, сформированный при создании запроса.

Сертификат может быть получен одним из двух способов:

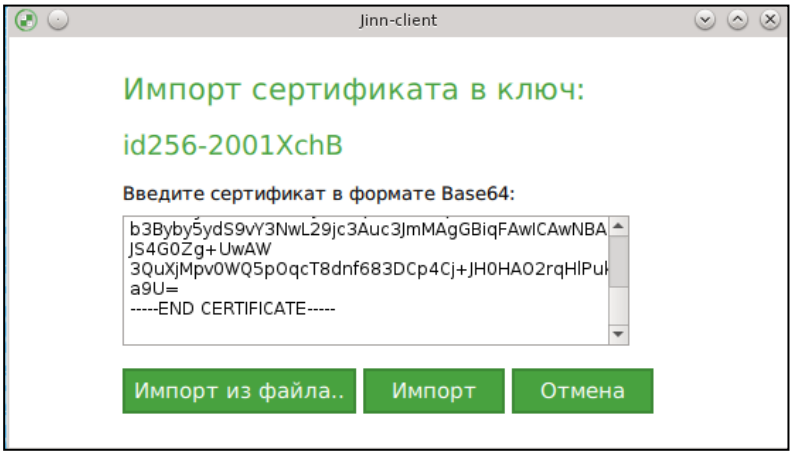
- на сайте УЦ копированием текста сертификата в формате Base64 через буфер обмена с сохранением на компьютере в каком-либо текстовом редакторе;
- в виде файла, полученного из УЦ.

Для записи сертификата на ключевой носитель:

1. Вставьте ключевой носитель с ключом, сформированным при создании запроса.
2. В главном окне Jinn-Client перейдите в раздел "Ключи и сертификаты".

   На экране появится список обнаруженных на носителе ключей.
3. Выберите ключ, которому должен соответствовать сертификат, и нажмите кнопку "Импортировать".

   На экране появится окно, предназначенное для импортирования сертификата.



4. Если сертификат был получен на сайте УЦ в формате Base64, откройте его в текстовом редакторе, скопируйте текст сертификата в форму для ввода (см. рисунок выше) и нажмите кнопку "Импорт".

   Если сертификат был получен в виде файла, нажмите кнопку "Импорт из файла..." и в открывающемся стандартном окне укажите путь к файлу.

   Будет выполнена запись сертификата на ключевой носитель.

Настройка работы с веб-порталом

Настройка включает в себя:

- установку и настройку расширения для веб-браузера;
- настройку окружения для работы с веб-порталом.

Внимание! Перед первым обращением к веб-порталу необходимо, чтобы после установки на компьютер Jinn-Client был запущен хотя бы один раз. Данное требование должно быть доведено до всех пользователей Jinn- Client, подписывающих документы на веб-портале.

Установка и настройка плагина

Предусмотрено два варианта установки плагина: скачиванием из интернет-магазина и локальной установкой.

Для скачивания из интернет-магазина:

1. Скачайте в интернет-магазине расширений для вашего браузера расширение Jinn Sign Extension и установите его.

   После успешной установки в правом верхнем углу окна браузера появится значок расширения Jinn Sign Extension. Зеленый цвет значка означает готовность к подписанию документов на веб-портале.
2. Если в качестве веб-браузера используется Google Chrome, в параметрах расширения Jinn Sign Extension установите отметку в поле "Разрешить открывать локальные файлы по ссылкам".

Для локальной установки:

1. Получите у компании "Код Безопасности" установочный пакет плагина.
2. Зайдите в настройки браузера, перейдите на вкладку расширений и нажмите "Установить расширение из файла".

   Появится стандартное окно выбора файла.
3. Выберите файл установочного пакета плагина.

   Будет выполнена установка плагина.

Внимание! Для корректной работы плагина Jinn Sign Extension необходимо убедиться, что в данный момент в браузере активна только одна его версия. Устаревшую версию (например, после обновления плагина) необходимо отключить или удалить.

Наличие двух активных плагинов отображается в области индикаторов расширений в правом верхнем углу браузера, а также в настройках расширений.

Для отключения или удаления плагина:

1. Зайдите в настройки расширений браузера.

   На вкладке отобразятся установленные плагины с указанием их версий.
2. Выберите устаревший плагин и, в зависимости от используемого браузера, отключите его или удалите.

Настройка окружения для работы с веб-порталом

Данная настройка выполняется в том случае, если установка браузера, используемого для работы с веб-порталами, была выполнена в папку, отличную от задаваемой по умолчанию.

Примечание. Jinn-Client для работы с веб-порталами поддерживает работу с браузерами Google Chrome и Mozilla Firefox.

- Если на компьютере был установлен браузер Google Chrome, скопируйте файл /opt/securitycode/jc2/web/manifests/chrome/ru.securitycode.jinn.sign.extension.provider.json в папку

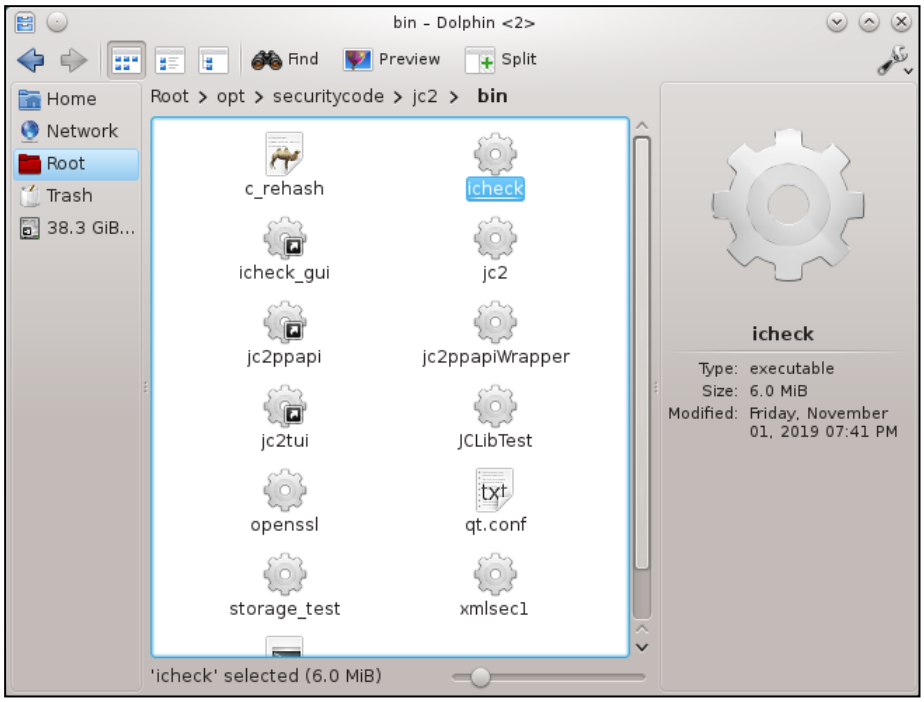
/home/user/.config/google-chrome/NativeMessagingHosts/.

- Если на компьютере был установлен браузер Mozilla Firefox (устанавливается в составе ОС Linux по умолчанию), скопируйте файл /opt/securitycode/jc2/web/manifests/firefox/ru.securitycode.jinn.sign.extension-.provider.json в папку /home/user/.mozilla/extensions/native- messaging-hosts/.

Приложение

Запуск процедуры контроля целостности вручную

Для проверки целостности файлов ПО Jinn-Client используется утилита **icheck**, хранящаяся в папке /opt/securitycode/jc2/bin.



Для запуска утилиты пользователь должен иметь права суперпользователя.

Запуск утилиты осуществляется в консольном терминале. При запуске можно использовать следующие ключи:

Ключ	Описание
-h (help)	Показать подсказку
-v (version)	Показать версию
-V (verbose)	Добавить вывод в консоль
-c (check)	Только проверка (не удалять ничего при ошибке КЦ)
-f (force)	Принудительная проверка (даже если не прошло 24 часа с момента последней проверки)
-i (integrity <integrity>)	Задать входной файл со списком файлов для КЦ
-o (output-file <output>)	Задать выходной файл, который будет создан при успехе
-l (log file <log>)	Задать файл, куда будут перенаправлены логи этой проверки

Для запуска процедуры контроля целостности:

1. Откройте консоль и перейдите в каталог /opt/securitycode/jc2/bin.
2. Введите команду запуска утилиты **icheck**, используя ключи, описанные выше.

   Будет выполнена проверка целостности файлов ПО Jinn-Client.

   В случае отрицательного результата проверки появится соответствующее сообщение. В этом случае необходимо переустановить Jinn-Client.

Параметры и пример конфигурационного файла libstorage.ini

Ниже в таблице приведены рабочие параметры конфигурационного файла libstorage.ini (см. стр.11).

Параметр	Значение
Base64Cert	Признак записи сертификата в Base64-кодировке для файлового ключевого контейнера, по умолчанию включен
PKCS#11	Список путей к файлам PKCS#11-библиотек для работы с носителями через PKCS#11-интерфейс, разделенных одним из символов «;», «,» или «|»
Directory	Список дополнительных директорий, где размещаются ключевые контейнеры, разделенные одним из символов «;», «,» или «|»
DefaultPIN	Признак использования PIN-кода по умолчанию некоторыми носителями, по умолчанию включен
DefaultPINCodes	Связанный список значений PIN-кодов по умолчанию с моделями устройств, работающими через PKCS#11-интерфейс, задается в виде набора строк, разделенных символом ';', вида: "Model=PIN"
IgnoreCryptoPro	Признак работы только с PKCS#15-контейнерами, исключающий выборку контейнеров КриптоПро, по умолчанию выключен
WriteCertModels	Список моделей устройств, работающих через PKCS#11-интерфейс, которые требуют авторизации пользователя при записи сертификата

Пример конфигурационного файла

// Признак записи сертификата в Base64 кодировке для файлового ключевого контейнера, по умолчанию включен

//Base64Cert=1

// Список путей к файлам PKCS#11-библиотек для работы с носителями через PKCS#11-интерфейс

//PKCS#11=rtPKCS11ECP.dll;jcPKCS11-2.dll;isbc_pkcs11_main.dll;rtPKCS11.dll

//PKCS#11=librtpkcs11ecp.so;libjcPKCS11- 2.so;libisbc_ pkcs11_ main.so;opensc-pkcs11.so

// Список дополнительных директорий, где размещаются ключевые контейнеры

//Directory=

// Признак использования PIN-кода по умолчанию некоторыми носителями, по умолчанию включён

//DefaultPIN=0

// Связанный список значений PIN-кодов по умолчанию с моделями устройств, работающими через PKCS#11-интерфейс,

// задается в виде набора строк, разделенных символом ';', вида: "Model=PIN"

//DefaultPINCodes=~default~=12345678;PRO=1234567890;eToken GOST-T=1234567890;JaCarta GOST 2.0=1234567890;JaCarta DS-S=1234567890;JaCarta Laser=11111111

// Признак работы только с PKCS#15-контейнерами, исключающий выборку контейнеров КриптоПро, по умолчанию выключен

//IgnoreCryptoPro=1

// Список моделей устройств, работающих через PKCS#11-интерфейс, которые требуют авторизации пользователя при записи сертификата

//WriteCertModels=eToken GOST;JaCarta GOST 2.0;JaCarta DS;ESMART Token

Документация

1. Программа доверенной визуализации и подписи Jinn-Client. Версия 2. Руководство пользователя.
2. Программа доверенной визуализации и подписи Jinn-Client. Версия 2. Руководство программиста.
3. Программа доверенной визуализации и подписи Jinn-Client. Версия 2. Руководство администратора.