КОД безопасности

Программа доверенной визуализации и подписи

Jinn-Client

Версия 2

Руководство пользователя

RU.АМБС.58.29.12.010 92

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 пользователей 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 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.

Функции пользователя

Основной функцией пользователя в Jinn-Client является подписывание документов электронной подписью с предварительным просмотром подписываемого документа. Кроме того, пользователь решает следующие задачи:

- Создание запроса на получение сертификата и запись полученного сертификата на ключевой носитель.

  Пользователь заполняет форму запроса и передает ее (самостоятельно или через администратора) в УЦ. Одновременно с созданием запроса формируется ключ. При этом пользователь сам задает пароль доступа к ключу.

  На основании запроса УЦ выпускает сертификат электронной подписи.

  После получения сертификата из УЦ пользователь записывает его на ключевой носитель.

  Примечание. Пользователь может получить у администратора ключевой носитель с записанными на него ключом и сертификатом. В этом случае пароль к ключу должен сообщить администратор.

- Копирование ключей на ключевые носители.

  При необходимости пользователь может скопировать имеющиеся у него ключи и сертификаты на другой ключевой носитель.

- Задание папки хранения подписанных документов.

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).

Принципы функционирования

Электронная подпись

Электронная подпись (ЭП) документа представляет собой данные в электронной форме, присоединяемые к подписываемому электронному документу. ЭП получается в результате криптографического преобразования информации с использованием ключа ЭП. Электронная подпись позволяет определить лицо, подписавшее электронный документ, а также установить наличие искажений информации в документе.

Правовые условия применения ЭП в электронных документах определяются положениями Федерального закона РФ "Об электронной подписи" от 06.04.2011 №63-ФЗ.

В настоящее время в корпоративной ИТ- инфраструктуре предприятий все большее распространение получают операционные системы (ОС) семейства Linux. На правительственном уровне принимаются нормативно-правовые документы по поддержке внедрения ОС семейства Linux в федеральных государственных учреждениях.

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	

Устройство	Примечание
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.

Сертификат ключа проверки ЭП

Сертификат ключа проверки электронной подписи — это цифровой документ, содержащий информацию о владельце сертификата, наименование удостоверяющего центра (УЦ) издателя сертификата, ключ проверки ЭП, сведения об области использования ключа проверки ЭП и т. д. Сертификат заверяется ЭП удостоверяющего центра.

Jinn-Client автоматически отслеживает статус сертификата — действителен или недействителен. Недействительным сертификат может быть признан по следующим причинам:

- срок действия сертификата не наступил;
- срок действия сертификата истек;
- отсутствует сертификат удостоверяющего центра.

Необходимо использовать только действительные сертификаты.

Сертификат может быть получен пользователем одним из двух способов:

1. Администратор передает пользователю ключевой носитель с записанными на него ключом и файлом сертификата. При этом администратор должен сообщить пользователю пароль доступа к ключу и PIN-код, если ключевой носитель защищен PIN-кодом.
2. Пользователь создает файл запроса на получение сертификата. Одновременно с файлом запроса формируется ключ и записывается на ключевой носитель пользователя.

   Пользователь передает администратору созданный запрос (файл с расширением .pem).

   На основании полученного от пользователя запроса администратор обращается в УЦ для выпуска сертификата.

   Выпущенный сертификат (файл с расширением .cer) администратор передает пользователю.

   Пользователь записывает файл сертификата на ключевой носитель.

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 раз в сутки;
- при запуске Jinn-Client, если проверка не выполнялась в течение последних 12 часов;
- вручную по команде администратора.

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

Настройки

Для работы пользователя в Jinn-Client необходимо, чтобы администратор выполнил следующие настройки:

- Установил лицензию на использование Jinn-Client.
- Настроил профили подписания.

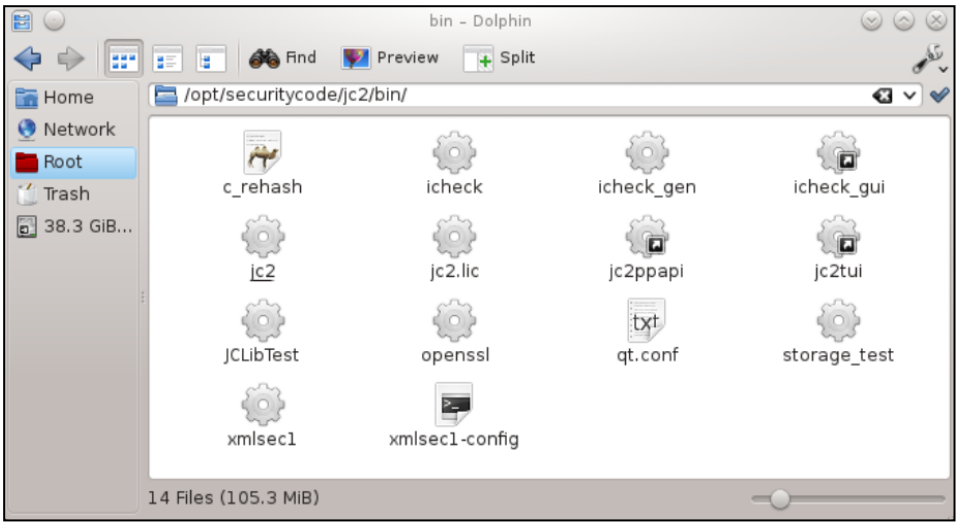
- При необходимости настроил параметры расширенного запроса на сертификат.
- Выдал пользователю ключевой носитель (носители) с ключами, сертификатами и паролями или проинформировал о необходимости создать запрос на получение сертификата.

Глава 2
Вызов Jinn-Client и описание главного окна

Вызов Jinn-Client

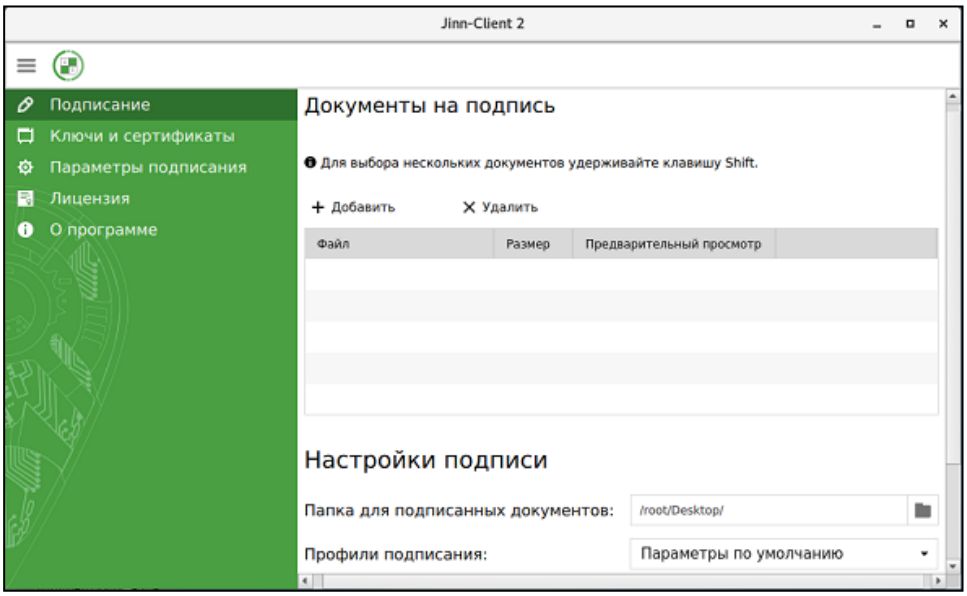
Для вызова Jinn-Client:

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



2. Запустите исполняемый файл jc2.

   На экране появится главное окно Jinn-Client.

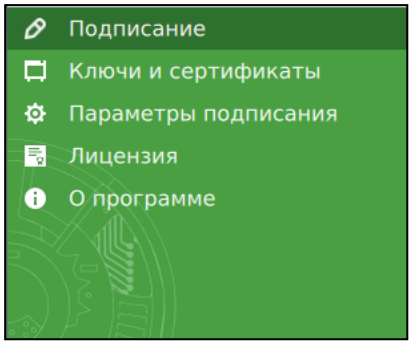


   Описание главного окна приведено в следующем подразделе.

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.

Глава 3
Работа с сертификатами в Jinn-Client

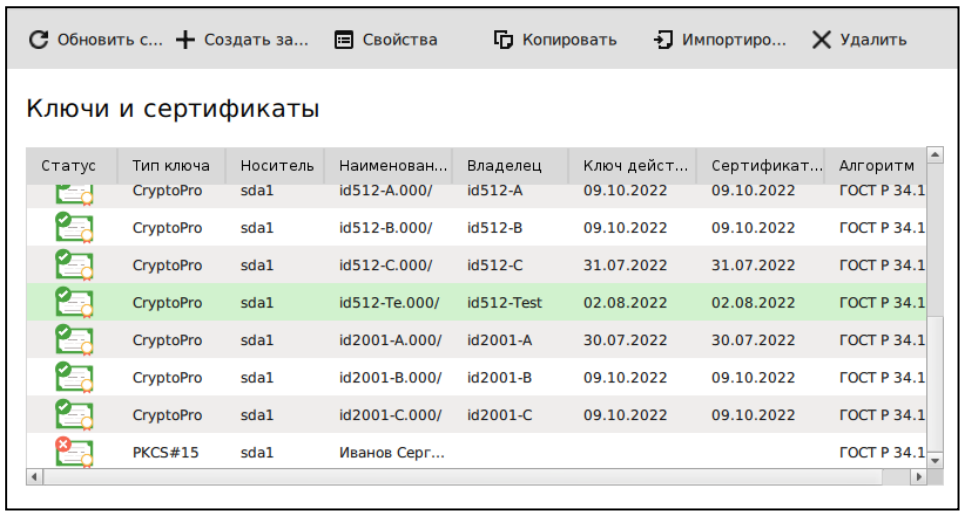
Просмотр сведений о ключах и сертификатах

Сведения о ключах и сертификатах пользователя отображаются в разделе "Ключи и сертификаты".

Для просмотра сведений:

- Вставьте ключевые носители и нажмите кнопку "Обновить список".

  Появится список всех обнаруженных ключей.



  Внимание! Ключи типа "CryptoPro" отображаются только при наличии расширенной лицензии.

Для каждого ключа приводится следующая информация:

- Статус — пиктограмма, предупреждающая об истечении срока действия сертификата или ключа.
- Тип ключа — PKCS#15 (формат компании "Код Безопасности", версия 4) или CryptoPro.
- Носитель — название ключевого носителя, на котором хранится ключ; название автоматически присваивается операционной системой при подключении носителя.
- Наименование ключа — наименование ключа, присваиваемое при его генерации и зависящее от типа ключевого носителя.
- Владелец — владелец сертификата.
- Срок действия ключа.
- Срок действия сертификата.
- Алгоритм — номер ГОСТа, в соответствии с которым сформирован ключ.

При просмотре списка ключей доступны следующие операции:

- создание запроса на получение сертификата;
- просмотр информации о сертификате;
- копирование ключа на другой ключевой носитель;
- импорт сертификата в ключ;
- удаление ключа с ключевого носителя.

Создание запроса на выпуск сертификата

Jinn-Client позволяет создать запрос формата PKCS#10 на выпуск сертификата ключа проверки ЭП.

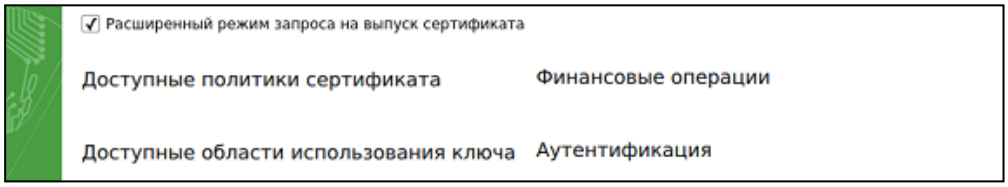
Запрос на выпуск сертификата создается пользователем Jinn-Client по мере необходимости. Одновременно с запросом будет создан ключ ЭП в криптографическом контейнере, при этом пользователь самостоятельно назначает пароль доступа к криптографическому контейнеру и задает разрядность ключа.

Создание запроса может выполняться по одному из двух сценариев:

- создание обычного запроса;
- создание расширенного запроса.

Второй сценарий отличается от первого действиями, в которых пользователь должен указать дополнительные сведения о запрашиваемом сертификате.

Сценарий, по которому создается запрос, настраивается администратором. Расширенный запрос создается в том случае, если в разделе "Настройки" в параметрах запроса на выпуск сертификата установлена отметка "Расширенный режим запроса на выпуск сертификата" (см. рисунок ниже).



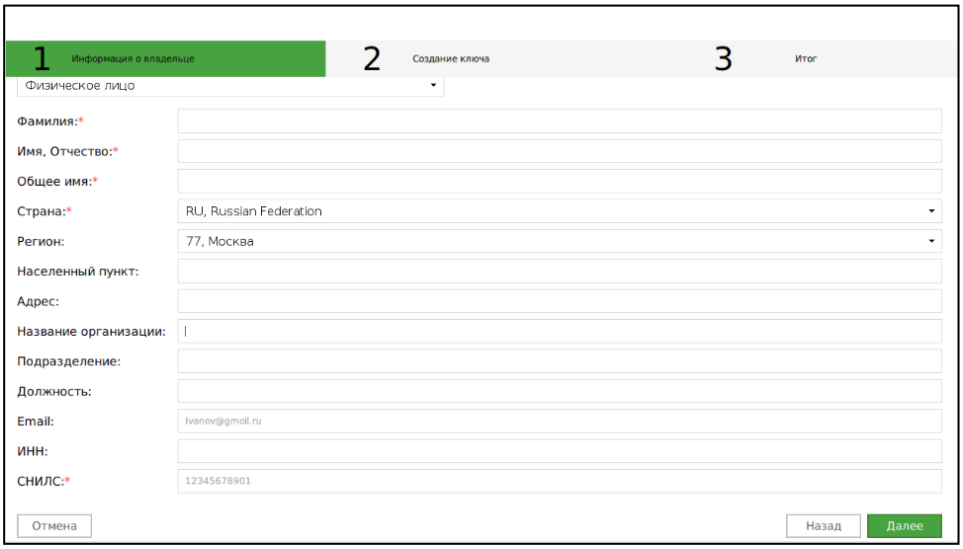
Созданный запрос на выпуск сертификата пользователь передает администратору безопасности, а ключ ЭП хранит у себя.

Создание обычного запроса

Для создания запроса:

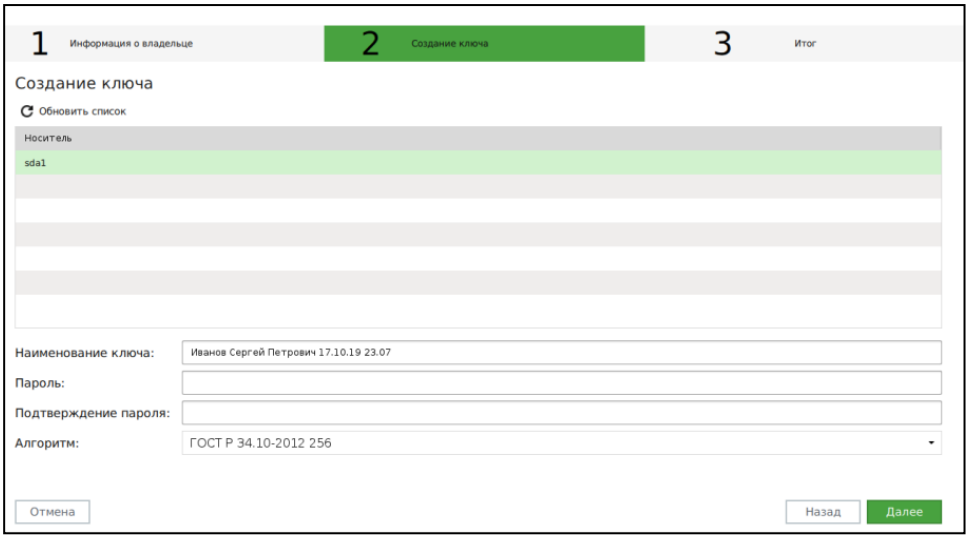
1. В главном окне Jinn-Client перейдите в раздел "Ключи и сертификаты" и нажмите кнопку "Создать запрос".

   На экране появится окно мастера генерации запроса на сертификат, предназначенное для ввода информации о владельце сертификата.



2. Укажите параметры владельца сертификата и нажмите кнопку "Далее >".

   На экране появится следующее окно мастера запроса на сертификат, предназначенное для создания ключа.



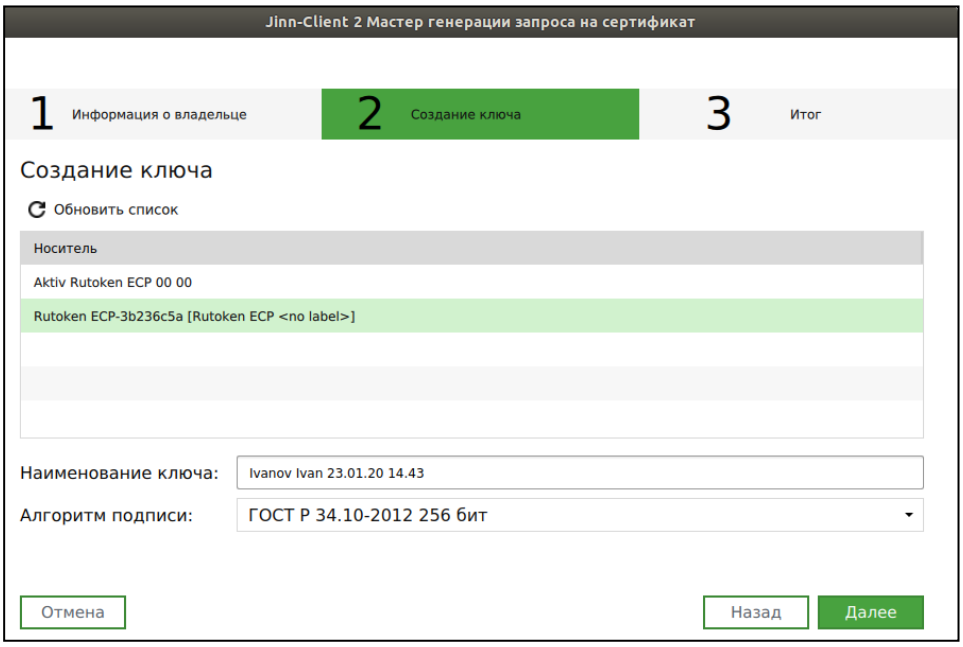
3. Вставьте ключевой носитель или носители, если их несколько, и нажмите кнопку "Обновить список".

Появится список предъявленных ключевых носителей.

Примечание. В некоторых операционных системах требуется предварительно выполнить монтирование устройства.

4. Выделите в списке ключевой носитель, на котором должен быть создан ключ и на который должен будет записан сертификат.

Если в качестве ключевого носителя используется электронный идентификатор (смарт-карта или USB-ключ), окно мастера примет следующий вид:



Перейдите к п. **6**.

Если в качестве ключевого носителя используется USB-флеш-накопитель, перейдите к п. **5**.

5. Введите и подтвердите пароль для доступа к ключу.

К паролю предъявляются следующие требования:

- Длина пароля должна составлять не менее 6 символов.
- В качестве символов должны использоваться хотя бы один из символов следующих групп:

- прописные латинские буквы A – Z;
- строчные латинские буквы a – z;
- арабские цифры 0 – 9;
- знаки препинания и спецсимволы (без кавычек) ":", ";", ",", ".", "<", ">", "?", "/", "{", "}", "[", "]".

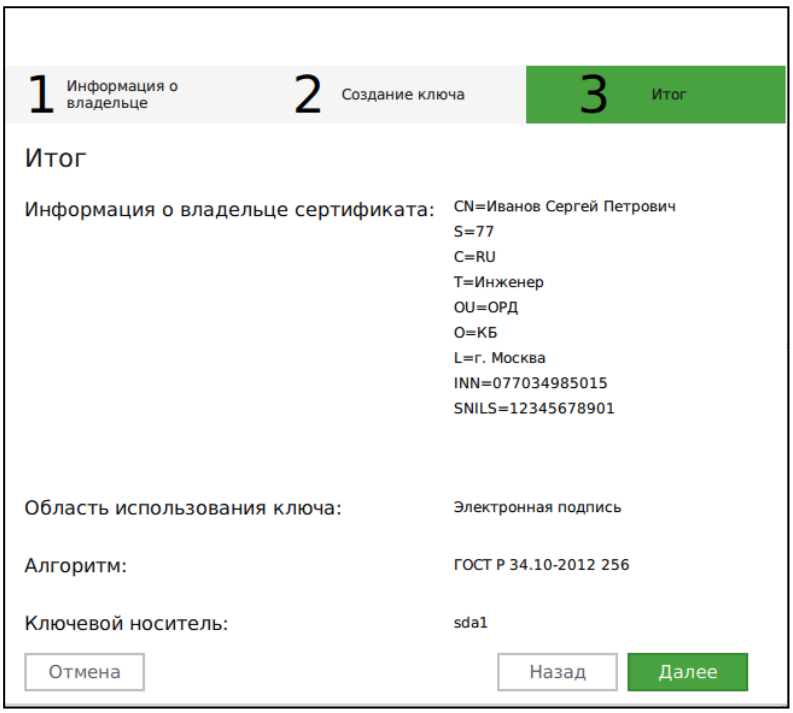
- При смене пароля не допускается повторное назначение одного и того же пароля.

Внимание! Запомните или запишите наименование ключа. Оно потребуется при записи сертификата на ключевой носитель.

6. Укажите требуемую разрядность ключа (256 или 512) и при необходимости измените наименование ключа, сгенерированное автоматически.

   Нажмите кнопку "Далее".

   На экране появится итоговое окно мастера.



7. Проверьте правильность отображаемых сведений и нажмите кнопку "Далее".

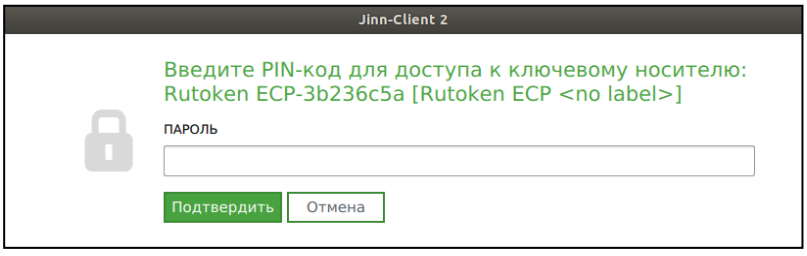
   Начнется процедура накопления энтропии для датчика случайных чисел.

   Внимание! При использовании физического датчика случайных чисел ПАК "Соболь" набор энтропии выполняется автоматически и на экране не отображается.

   При использовании биологического датчика случайных чисел на экране появится окно накопления энтропии.

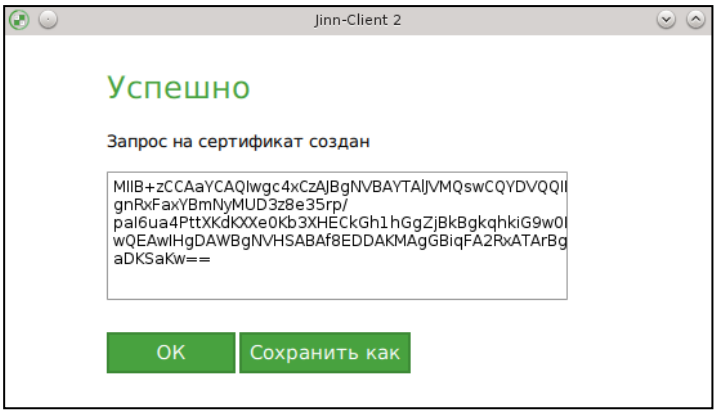
8. Следуйте отображаемой в окне инструкции, стараясь попасть в мишень, и дождитесь завершения набора энтропии.

   Если в качестве ключевого носителя используется электронный идентификатор, на экране появится окно ввода PIN-кода.



   Введите PIN-код и нажмите кнопку "Подтвердить".

На экране появится окно с сообщением об успешном завершении создания запроса.



Текст сформированного запроса отображается в окне в формате Base64 (см. рисунок выше).

9. Нажмите кнопку "Сохранить как".

   Появится стандартное окно сохранения файла.

10. Укажите папку, в которую должен быть сохранен файл запроса, задайте имя файла и нажмите кнопку "Сохранить".

    Файл будет сохранен в формате Base64 в указанную папку. Данный файл запроса можно передать в удостоверяющий центр для получения сертификата.

11. Нажмите кнопку "OK" в окне с сообщением об успешном завершении создания запроса (см. рисунок выше).

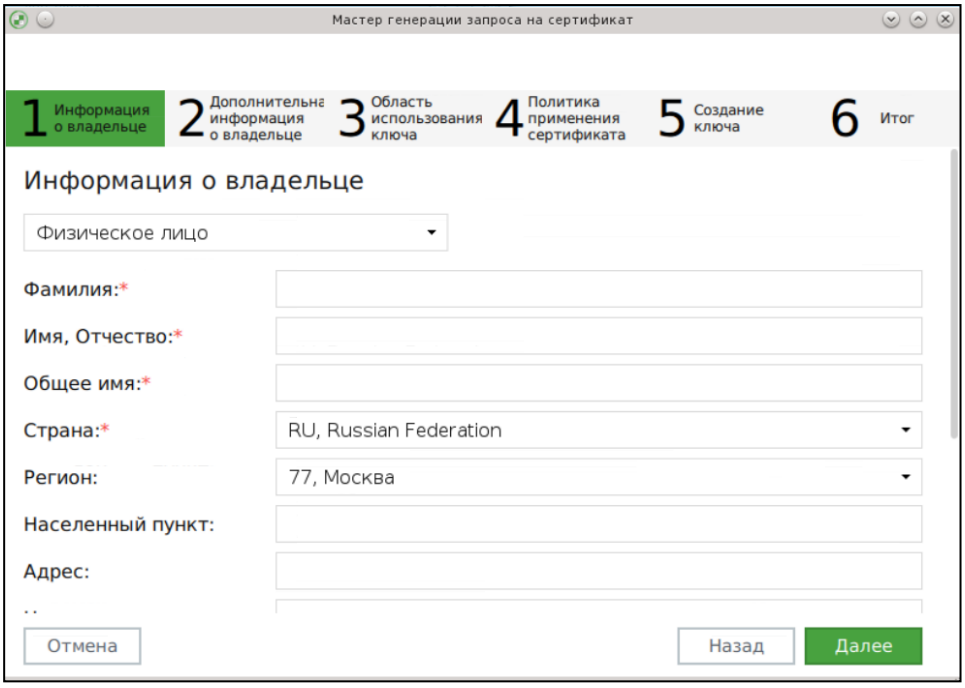
    Окно закроется и в списке ключей, обнаруженных на ключевом носителе, появится новая запись, соответствующая созданному запросу на выпуск сертификата. Новая запись будет выделена красным цветом.

Создание расширенного запроса

Для создания запроса:

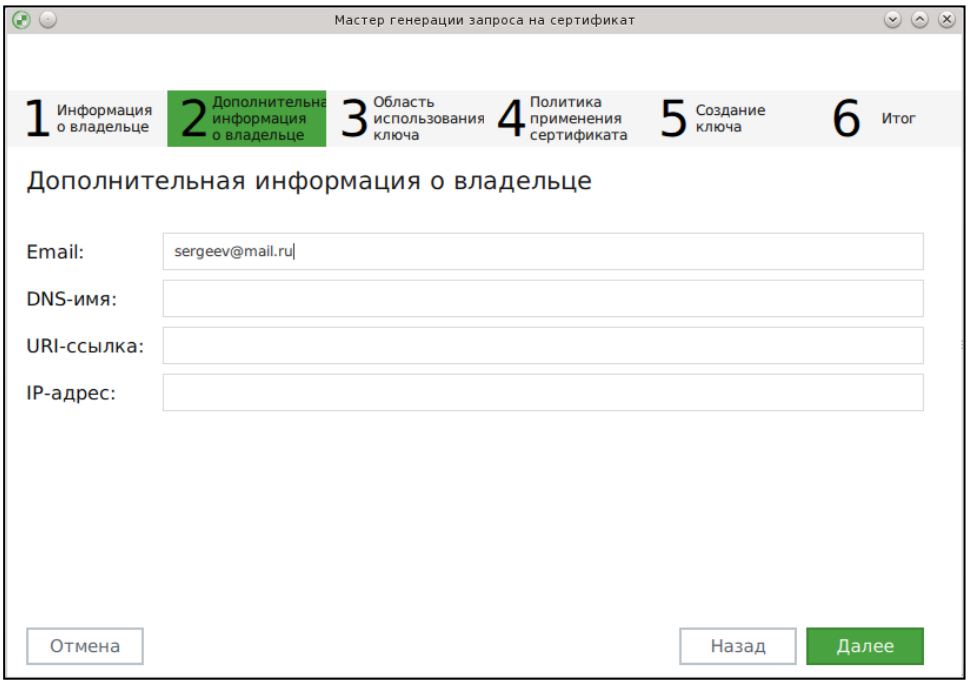
1. В главном окне Jinn-Client перейдите в раздел "Ключи и сертификаты" и нажмите кнопку "Создать запрос".

   На экране появится окно мастера генерации запроса на сертификат, предназначенное для ввода информации о владельце сертификата.



2. Укажите параметры владельца сертификата и нажмите кнопку "Далее >".

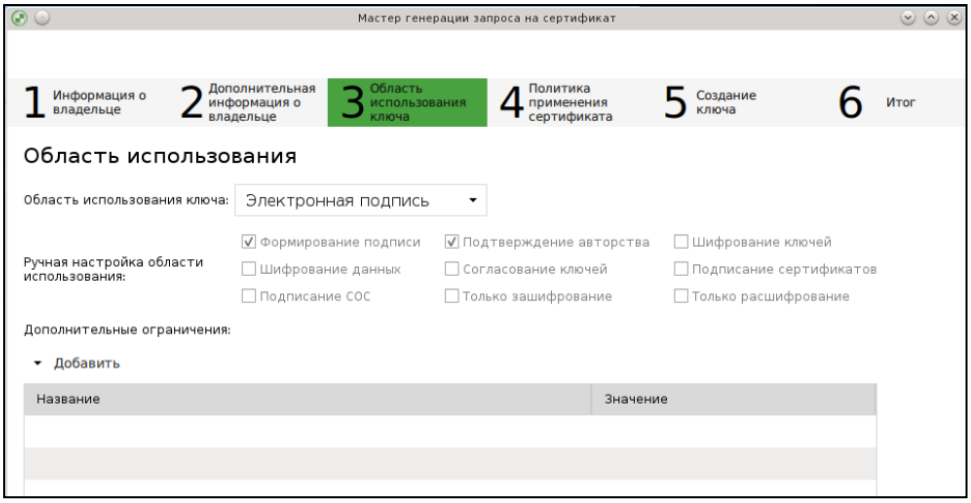
   На экране появится следующее окно мастера запроса на сертификат, предназначенное для ввода дополнительных сведений о владельце.



   Поля этого окна не являются обязательными и заполняются только по специальному требованию администратора.

3. Нажмите кнопку "Далее".

   На экране появится следующее окно мастера, предназначенное для задания области использования ключа и дополнительных ограничений.

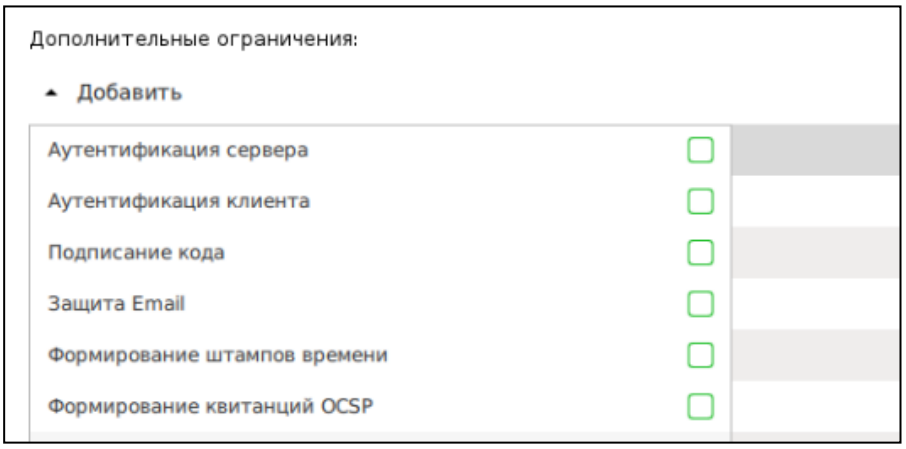


В поле "Область использования ключа" выберите значение "Электронная подпись" (устанавливается по умолчанию).

Примечание. Если требуется сформировать ключ с другой областью использования, выберите ее из списка. Если ни одна из них не подходит, выберите значение "Ручная настройка" и далее в разделе "Ручная настройка области использования" установите необходимые отметки.

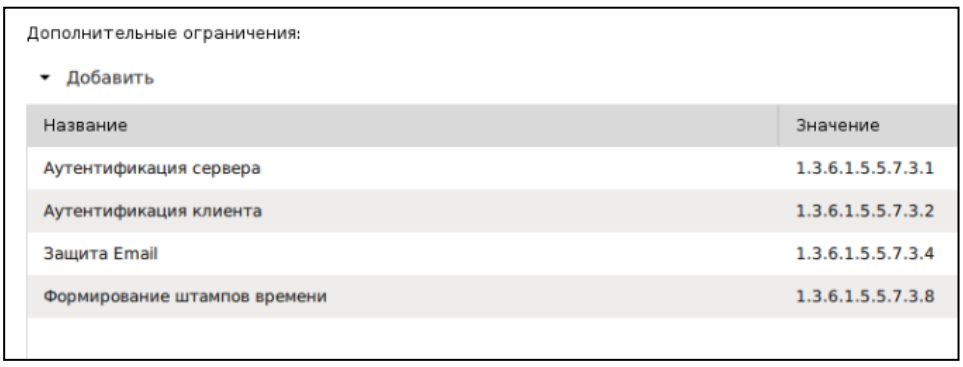
4. При необходимости укажите дополнительные ограничения. Для этого нажмите кнопку "Добавить".

   Появится список дополнительных атрибутов (расширений, которые можно включить в сертификат).



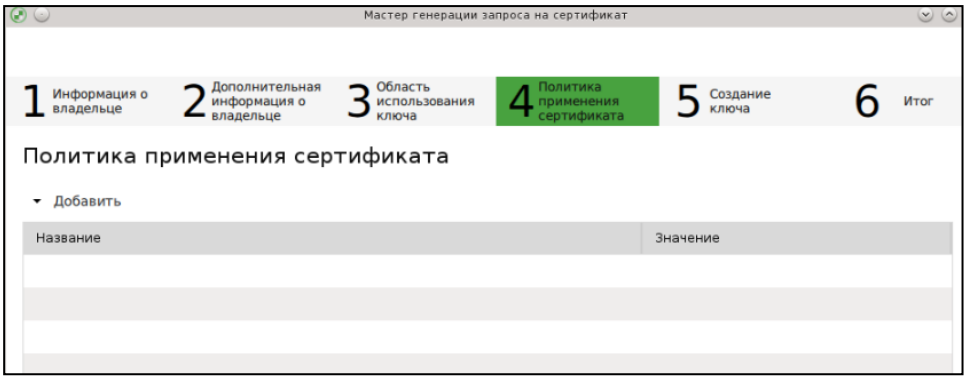
5. Установите отметки у тех атрибутов, которые необходимо включить в сертификат, и закройте список.

   В списке дополнительных ограничений появятся названия расширений и значения их OID.



6. Нажмите кнопку "Далее" в правом нижнем углу окна.

Откроется следующее окно мастера, предназначенное для задания политики применения сертификата.

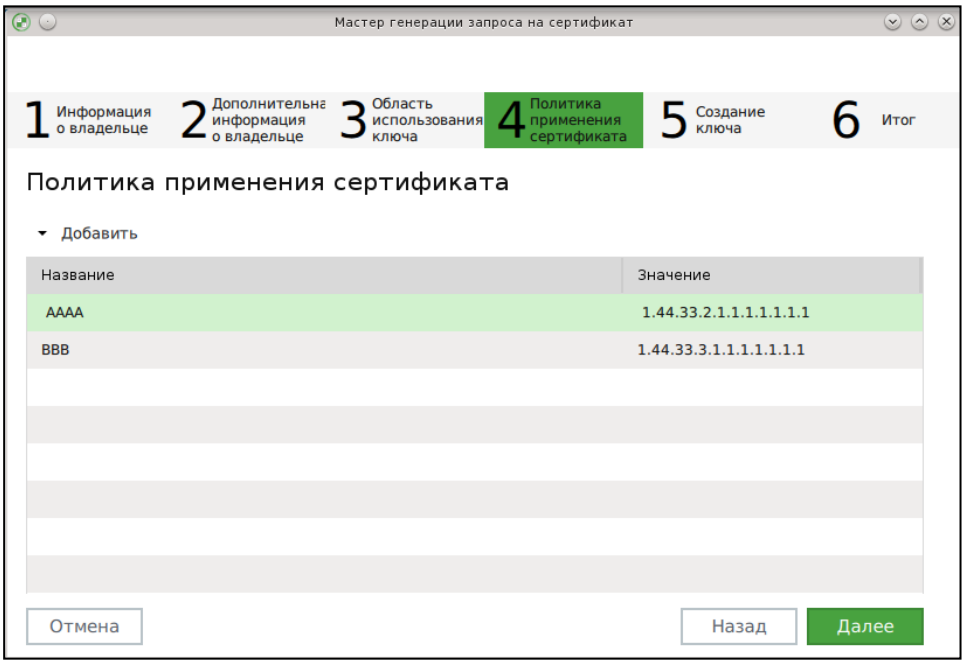


7. Нажмите кнопку "Добавить".

   Появится список дополнительных атрибутов (расширений, которые можно включить в сертификат).

8. Установите отметки у тех атрибутов, которые необходимо включить в сертификат, и закройте список.

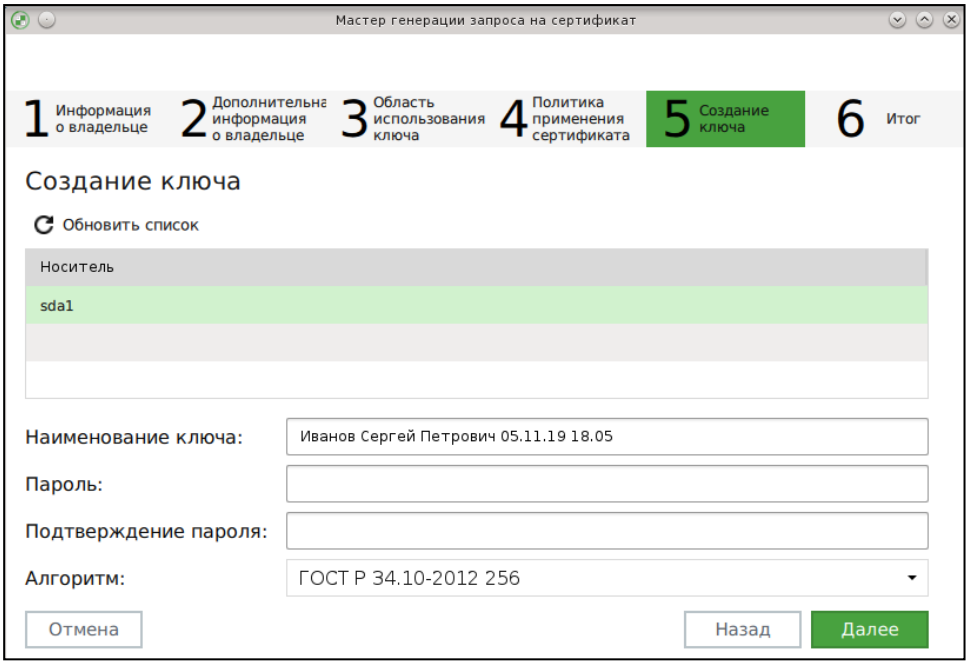
   В списке "Политика применения сертификата" появятся названия расширений и значения их OID.



9. Вставьте ключевой носитель или носители, если их несколько, и нажмите кнопку "Далее".

   Примечание. В некоторых операционных системах требуется предварительно выполнить монтирование устройства.

   Появится следующее окно мастера.



10. При необходимости нажмите кнопку "Обновить список".

В списке отобразятся все обнаруженные ключевые носители.

11. Выделите в списке ключевой носитель, на котором должен быть создан ключ и на который должен быть записан сертификат.

Если в качестве ключевого носителя используется электронный идентификатор (смарт-карта или USB-ключ), поля "Пароль" и "Подтверждение пароля" станут недоступны. В этом случае перейдите к п. **13**.

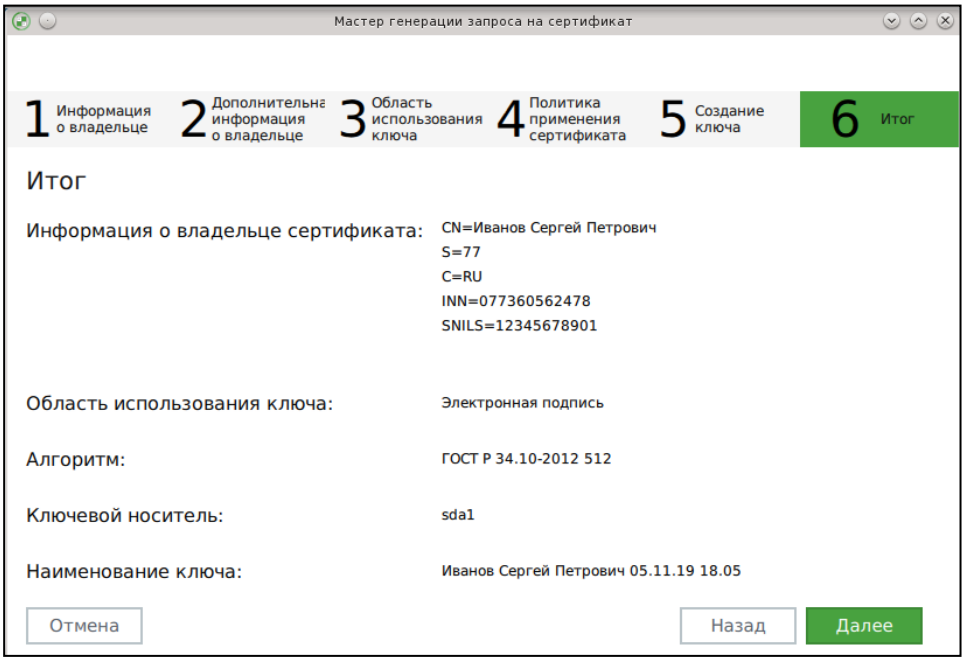
12. Введите и подтвердите пароль для доступа к ключу. Требования к паролю см. на стр.**16**.

Внимание! Запомните или запишите наименование ключа. Оно потребуется при записи сертификата на ключевой носитель.

13. Укажите требуемую разрядность ключа (256 или 512) и при необходимости измените наименование ключа, сгенерированное автоматически.

Нажмите кнопку "Далее".

На экране появится итоговое окно мастера.



14. Проверьте правильность отображаемых сведений и нажмите кнопку "Далее".

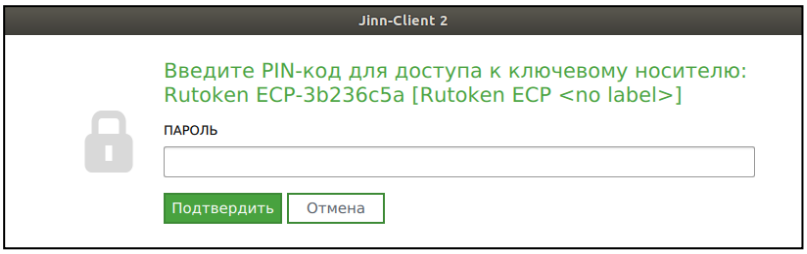
    Начнется процедура накопления энтропии для датчика случайных чисел.

    Внимание! При использовании физического датчика случайных чисел ПАК "Соболь" набор энтропии выполняется автоматически и на экране не отображается.

    При использовании биологического датчика случайных чисел на экране появится окно накопления энтропии.

15. Следуйте отображаемой в окне инструкции, стараясь попасть в мишень, и дождитесь завершения набора энтропии.

    Если в качестве ключевого носителя используется электронный идентификатор, на экране появится окно ввода PIN-кода.



    Введите PIN-код и нажмите кнопку "Подтвердить".

    На экране появится окно с сообщением об успешном завершении создания запроса (см. рисунок на стр.**18**).

    Текст сформированного запроса отображается в окне в формате Base64.

16. Нажмите кнопку "Сохранить как".

    Появится стандартное окно сохранения файла.

17. Укажите папку, в которую должен быть сохранен файл запроса, задайте имя файла и нажмите кнопку "Сохранить".

    Файл будет сохранен в формате Base64 в указанную папку. Данный файл запроса можно передать в удостоверяющий центр для получения сертификата.

18. Нажмите кнопку "ОК" в окне с сообщением об успешном завершении создания запроса.

    Окно закроется, и в списке ключей, обнаруженных на ключевом носителе, появится новая запись, соответствующая созданному запросу на выпуск сертификата. Новая запись будет выделена красным цветом.

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:

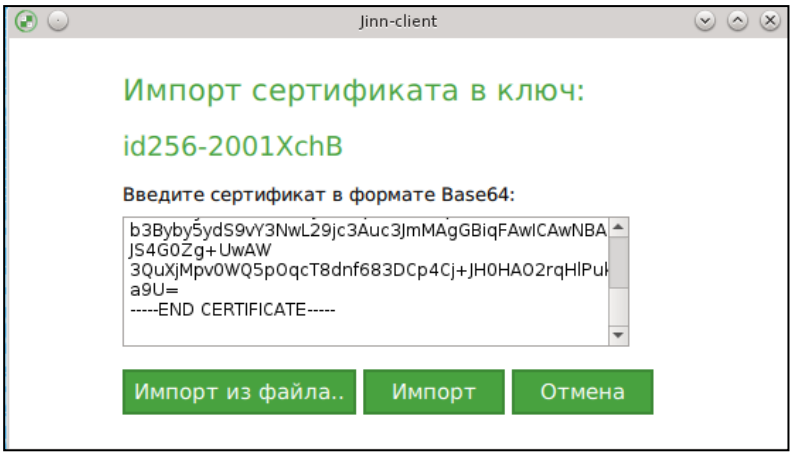
- на сайте УЦ копированием текста сертификата в формате Base64 через буфер обмена с сохранением на компьютере в каком-либо текстовом редакторе;
- в виде файла, полученного из УЦ.

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.

Просмотр информации о сертификате

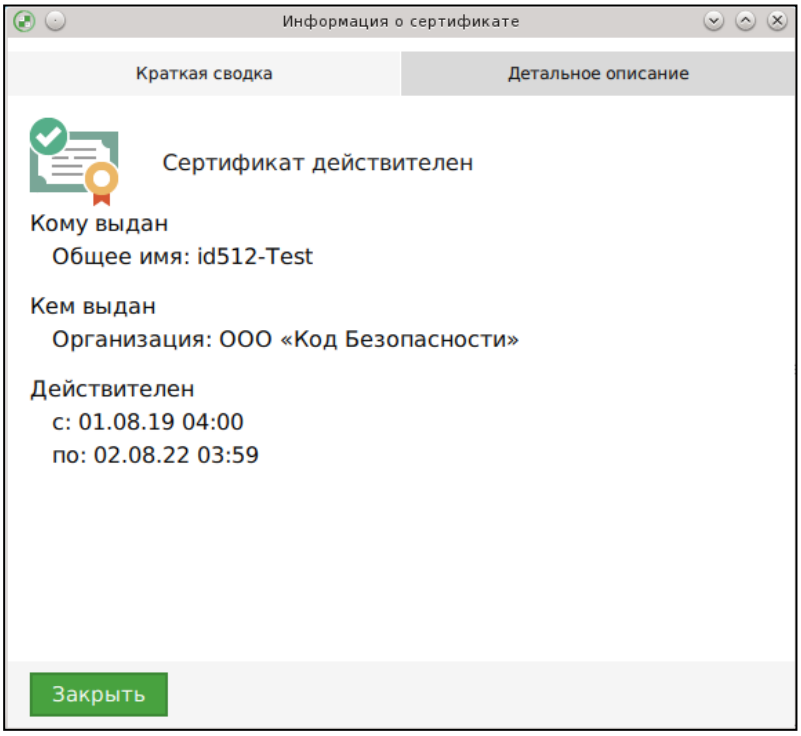
Для просмотра информации:

1. Вставьте ключевые носители и нажмите кнопку "Обновить список".

   Появится список всех обнаруженных ключей.

2. Выберите ключ и нажмите кнопку "Свойства".

   На экране появится окно "Информация о сертификате".



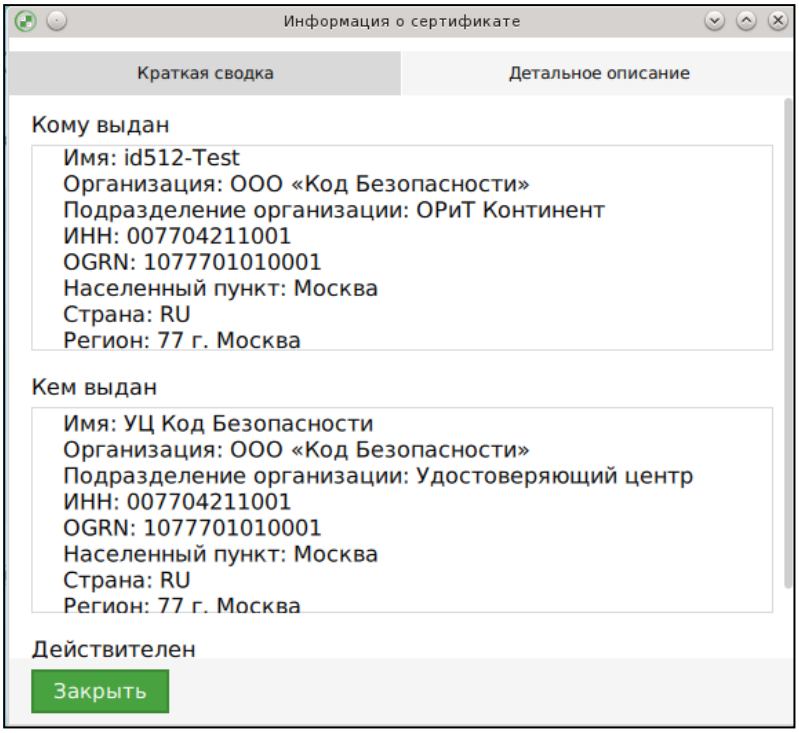
Окно содержит две вкладки: "Краткая сводка" и "Детальное описание".

На вкладке "Краткая информация" представлены следующие сведения:

- статус сертификата;

- кому и кем выдан;
- срок действия.

3. Для просмотра подробных сведений перейдите на вкладку "Детальное описание".



4. После просмотра информации нажмите кнопку "Закрыть".

Копирование ключа на ключевой носитель

При необходимости ключ формата PKCS#15 можно скопировать на другой ключевой носитель.

Для копирования ключа с USB-флеш-накопителя:

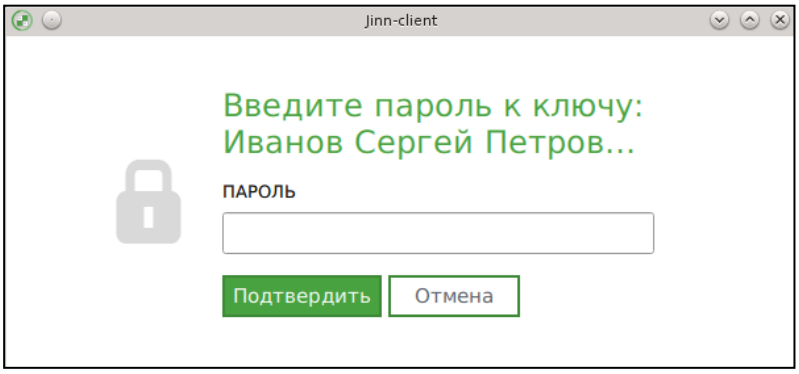
1. Вставьте ключевой носитель, с которого необходимо скопировать ключ, и ключевой носитель, на который требуется скопировать ключ.

   Нажмите кнопку "Обновить список".

   Появится список всех обнаруженных на носителях ключей.

2. Выберите ключ, предназначенный для копирования, и нажмите кнопку "Копировать".

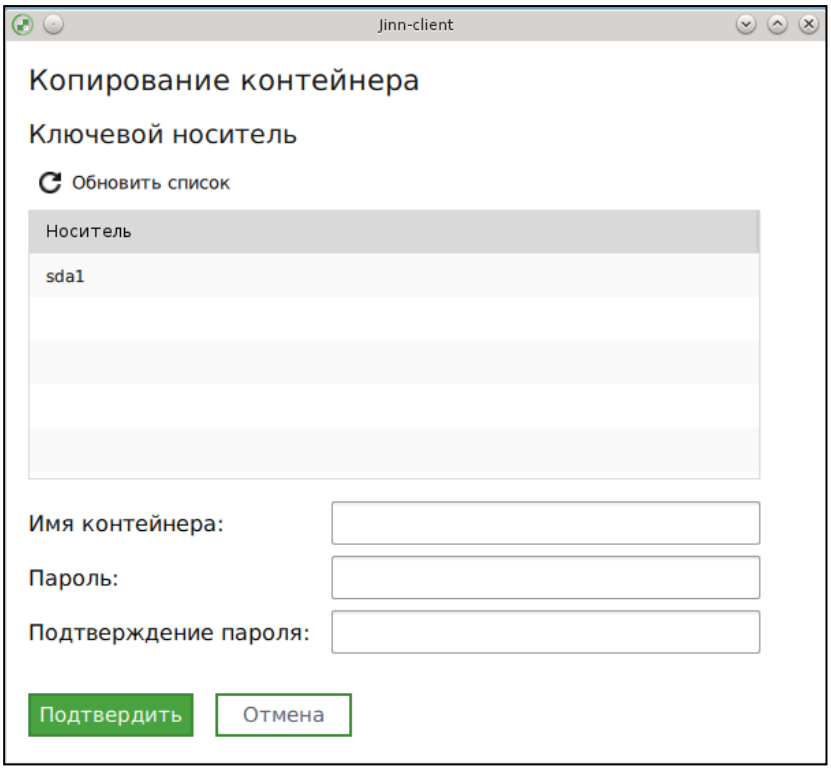
   На экране появится запрос на ввод пароля к копируемому ключу.



3. Введите пароль и нажмите кнопку "Подтвердить".

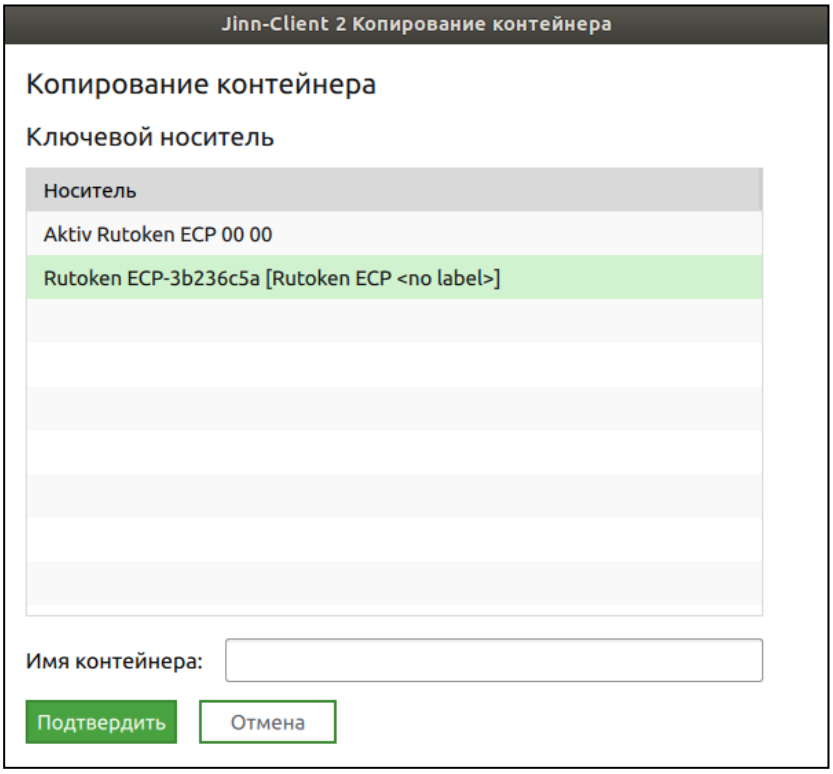
   Внимание! После 3 неудачных попыток ввода пароля использование ключа будет заблокировано на 30 минут.

На экране появится окно "Копирование контейнера".



4. Выберите носитель, на который должен быть скопирован ключ.

   Если носителем, на который должен быть скопирован ключ, является электронный идентификатор (смарт-карта или USB-ключ), вид окна "Копирование контейнера" изменится:



5. Если ключ копируется на USB-флеш-накопитель, назначьте и подтвердите пароль доступа к ключу. Запомните пароль. Требования к паролю см. на стр.**16**.

В поле "Имя контейнера" введите имя ключа, используя буквы латинского алфавита и цифры. Имя не должно совпадать с именем копируемого ключа.

Нажмите кнопку "Подтвердить".

Начнется запись ключа и сертификата на ключевой носитель.

Перейдите к п.**8**.

6. Если ключ копируется на электронный идентификатор (смарт-карту или USB-ключ), в поле "Имя контейнера" введите имя ключа (см. п. **5**) и нажмите кнопку "Подтвердить".

   На экране появится окно ввода PIN-кода.

7. Введите PIN-код и нажмите кнопку "OK".

   Начнется запись ключа и сертификата на ключевой носитель.

8. Дождитесь сообщения об успешном завершении операции копирования.

Для копирования ключа с электронного идентификатора:

1. Вставьте ключевой носитель, с которого необходимо скопировать ключ, и ключевой носитель, на который требуется скопировать ключ.

   Нажмите кнопку "Обновить список".

   Появится список всех обнаруженных на носителях ключей.

2. Выберите ключ, предназначенный для копирования, и нажмите кнопку "Копировать".

   На экране появится запрос на ввод PIN-кода электронного идентификатора.

3. Введите PIN-код и нажмите кнопку "Подтвердить".

4. Выберите в списке ключевой носитель, на который требуется скопировать ключ.

   - Если выбранным ключевым носителем является электронный идентификатор, на экране появится запрос на ввод PIN-кода.

     Введите PIN-код и далее в поле "Имя контейнера" введите новое имя ключа. Имя не должно совпадать с именем копируемого ключа.

     Примечание. Если ключ копируется на тот же носитель, на котором хранится копируемый, PIN-код вводить не требуется.

   - Если выбранным ключевым носителем является USB-флеш-накопитель, введите новое имя ключа, задайте и подтвердите пароль.

5. В окне "Копирование контейнера" нажмите кнопку "Подтвердить".

   Начнется запись ключа и сертификата на ключевой носитель.

6. Дождитесь сообщения об успешном завершении операции копирования.

Удаление ключа с ключевого носителя

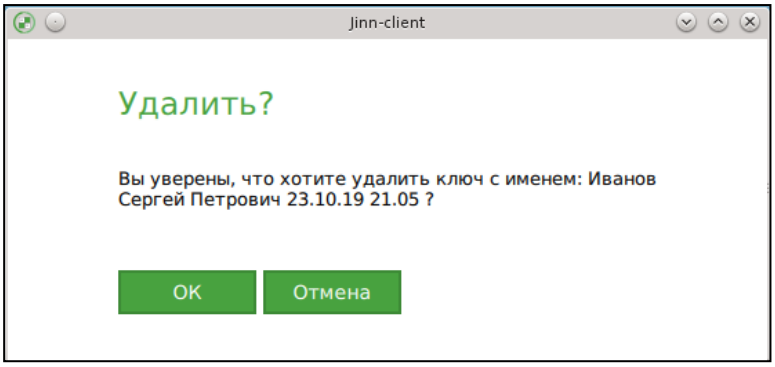
Для удаления ключа:

1. Вставьте ключевой носитель, с которого необходимо удалить ключ, и нажмите кнопку "Обновить список".

   Появится список всех обнаруженных ключей, записанных на носителе.

2. Выберите ключ, предназначенный для удаления, и нажмите кнопку "Удалить".

   На экране появится запрос на подтверждение выполнения операции удаления.



3. Нажмите кнопку "OK".
   Ключ будет удален с ключевого носителя.

Глава 4
Формирование электронной подписи в Jinn-Client

Подписание документов может осуществляться локально после вызова Jinn-Client или на веб-портале.

Для подписания документов электронной подписью пользователь должен иметь ключевой носитель с хранящимися на нем ключами и сертификатами.

Перед началом подписания документов необходимо выполнить настройки:

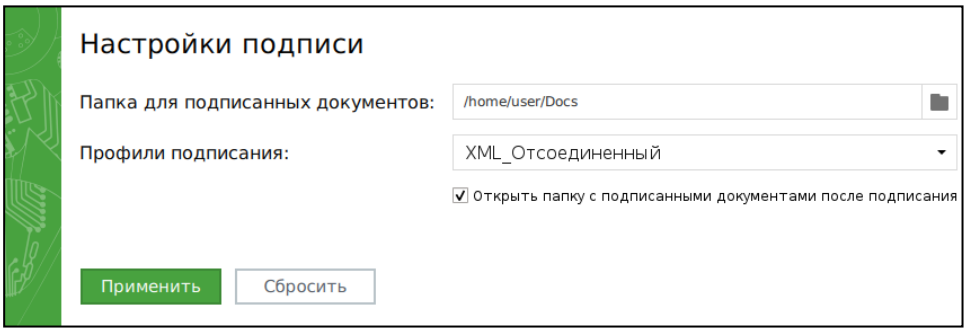
- Указать папку, в которую будут помещаться подписанные документы.
- Выбрать профиль подписания, настроенный администратором.
- Указать — следует ли открыть папку с подписанными документами после подписания.

Настройки подписи

Для настройки:

1. В главном окне Jinn-Client перейдите в раздел "Подписание".

   В нижней части окна отображаются настройки подписи.



2. При необходимости измените папку для подписанных документов. Для этого нажмите кнопку, расположенную справа, и выберите папку.
3. Выберите из раскрывающегося списка профиль подписания. Список содержит профиль по умолчанию и профили, созданные администратором (подробнее о профилях см. [**3**]).
4. Установите отметку, если необходимо открыть папку с подписанными документами после подписания.

Подписание документов

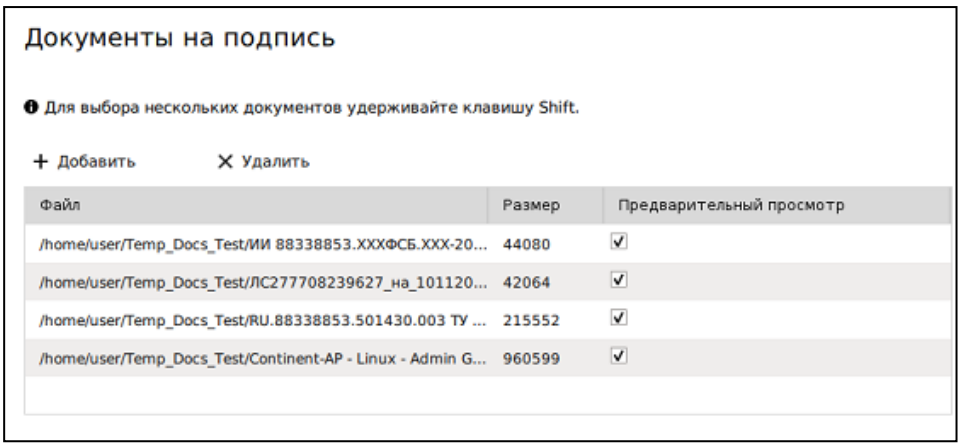
При подписании документов используются настройки, описанные выше. Если ни один из имеющихся профилей не подходит, его можно создать и добавить в список (о создании профилей см. [**3**]).

Подписание осуществляется ключом, имеющим действующий сертификат.

Для подписания документов:

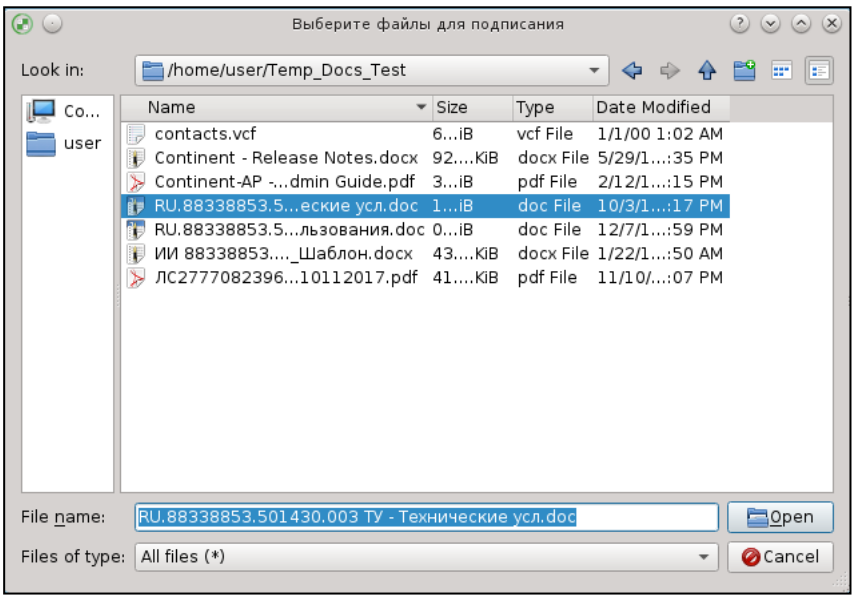
1. В главном окне Jinn-Client перейдите в раздел "Подписание".

   Верхняя часть окна предназначена для формирования списка документов, подлежащих подписанию. Профиль подписания, указанный в настройках, будет применен ко всем документам списка.



2. Для добавления документа в список нажмите кнопку "Добавить".

   На экране появится стандартное окно выбора файла.



3. Выберите документ и нажмите кнопку "Открыть".

   Выбранный документ появится в списке документов на подпись.

4. Добавьте в список другие документы.

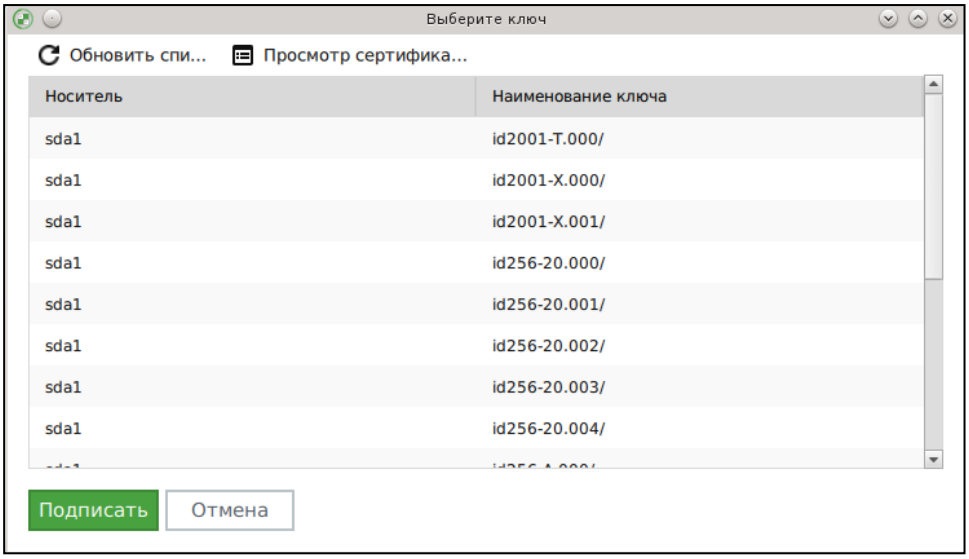
   По умолчанию при добавлении документа в список устанавливается отметка "Предварительный просмотр". Это означает, что перед подписанием содержание документа будет выведено на экран для просмотра. Если просмотр документа не требуется, удалите отметку.

   - Для удаления документа из списка выделите его и нажмите кнопку "Удалить".
   - Для очистки списка нажмите кнопку "Сбросить" в нижней части окна.

5. После формирования списка документов проверьте еще раз настройки подписи (см. стр.**29**) и при необходимости внесите требуемые изменения.

6. Вставьте носитель (носители) с ключами и нажмите кнопку "Подписать" в нижней части окна.

   На экране появится окно со списком обнаруженных ключевых носителей и хранящихся на них ключей.

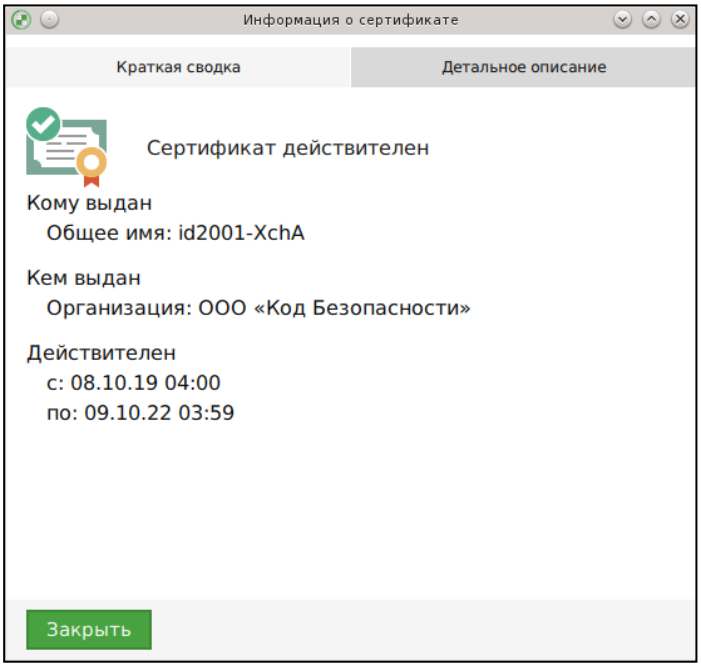


Примечание. Если список ключей не отображается, нажмите кнопку "Обновить список".

7. Выберите в списке ключ, которым предполагается подписать документы, и нажмите кнопку "Просмотр сертификата".

   Внимание! Запомните или запишите наименование ключа, которым будет выполнено подписание. Это потребуется для восстановления ключа при возникновении нештатной ситуации. О восстановлении ключа см. стр.**35**.

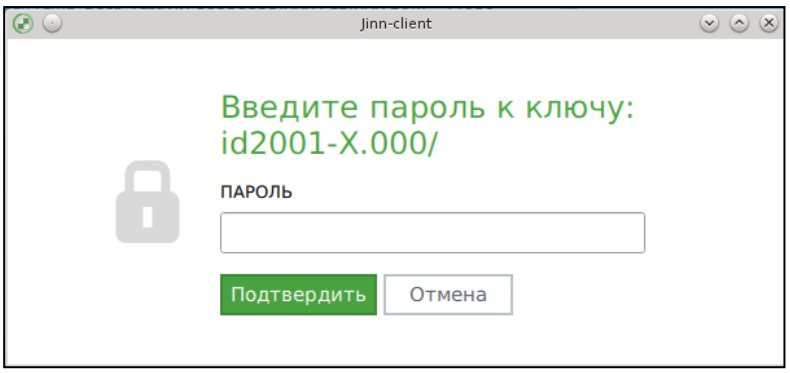
   На экране появится окно с информацией о сертификате.



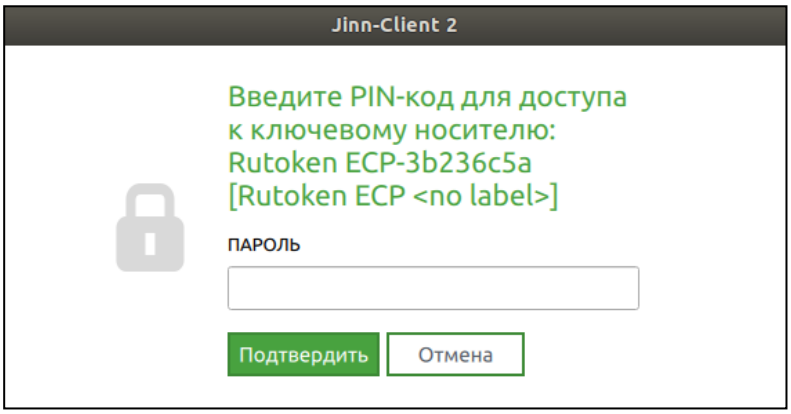
Примечание. Если у ключа отсутствует сертификат появится соответствующее сообщение. Использовать данный ключ нельзя.

   Окно с информацией о сертификате имеет две вкладки: "Краткая сводка" и "Детальное описание".

8. Ознакомьтесь с содержанием сертификата и нажмите кнопку "Закрыть".
9. Нажмите кнопку "Подписать".
   - Если в качестве ключевого носителя используется USB-флеш-накопитель, на экране появится запрос на ввод пароля ключа.



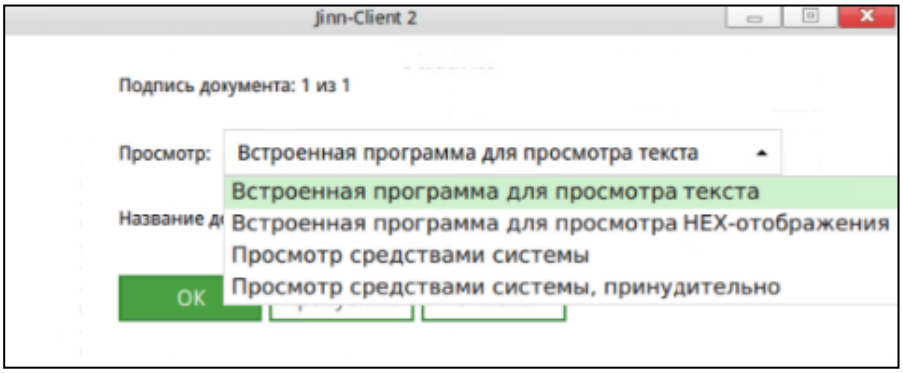
- Если в качестве ключевого носителя используется электронный идентификатор (смарт-карта или USB-ключ), на экране появится запрос на ввод PIN-кода.



10. Введите пароль или PIN-код и нажмите кнопку "Подтвердить".

Начнется последовательное подписание документов.

- Если у документа был установлен предварительный просмотр, на экране отобразится окно выбора программы просмотра документа.



В поле "Просмотр" выберите из раскрывающегося списка вариант просмотра документа. Доступны следующие варианты:

- Встроенная программа для просмотра текста — просмотр документа средствами ПО Jinn-Client.
- Встроенная программа для просмотра HEX-отображения — просмотр документа средствами ПО Jinn-Client в HEX-отображении.
- Просмотр средствами системы — приложение, в котором открывается документ для просмотра, определяется операционной системой в соответствии с настройками mime-типов. После подписания документа приложение закрывается.

Примечание. Просмотр средствами системы может не работать на некоторых ОС.

- Просмотр средствами системы, принудительно — приложение, в котором открывается документ для просмотра, определяется операционной системой. После подписания документа приложение остается открытым. Данный вариант используется в случае некорректной настройки библиотеки mime-типов.

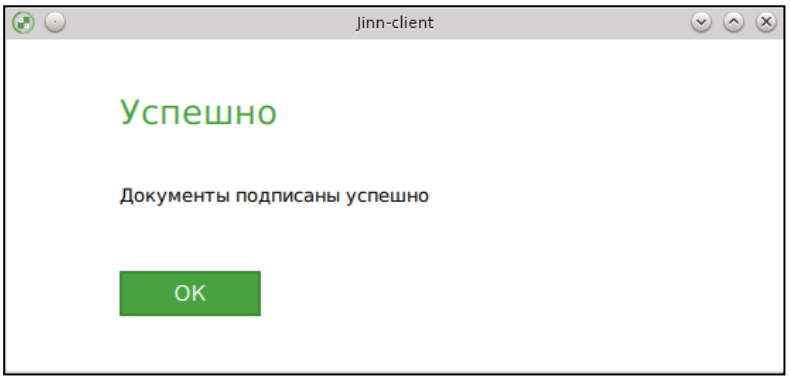
Внимание! Последние два варианта не являются режимами доверенной визуализации.

Примечание. При просмотре документа доступно его редактирование, но изменения в подписанный документ не войдут.

Просмотрите документ и нажмите кнопку "OK".

- Если для документа не предусмотрен предварительный просмотр, он будет подписан автоматически.

После успешного подписания всех документов на экране появится соответствующее сообщение.



11. Нажмите кнопку "OK".

Окно сообщения закроется и на экране появится окно с содержимым папки для подписанных документов. К названиям файлов подписанных документов добавляется расширение **.sig**.

Подписание на веб-портале

Для связи с веб- порталом и подписания документов используются установленные на компьютере пользователя веб-браузеры Google Chrome, Mozilla Firefox или Chromium и специализированный плагин. Плагин обеспечивает взаимодействие п API браузера с Jinn-Client.

Внимание! Перед первым обращением к веб-порталу необходимо, чтобы после установки на компьютер Jinn-Client был запущен хотя бы один раз.

Последовательность и содержание действий, выполняемых пользователем при подписании документов, зависит от сценариев, предусмотренных разработчиками веб-портала.

В общем случае для подписания документов необходимо выполнить следующее:

1. Используя браузер, зайдите на страницу веб-портала, предназначенную для подписания документов.
2. На странице веб-портала выберите документ или несколько документов для подписания.
3. Укажите параметры подписания, если это предусмотрено. Например:
   - включить документ в подпись;
   - включить сертификат в подпись;
   - отображать результат выполненной операции и пр.
4. Вставьте ключевой носитель или ключевые носители, если планируется использовать разные ключи.
5. Вызовите процедуру подписания.

На компьютере пользователя будет запущен Jinn-Client (если до этого он не был запущен) и на экране появится список обнаруженных ключей.

Внимание! Если после вызова процедуры подписания ничего не происходит, убедитесь, что на экране компьютера нет блокирующего окна с сообщением о том, что Jinn-Client работает уже 24 часа и для продолжения дальнейшей работы необходимо перезагрузить Jinn-Client. Если окно присутствует, нажмите в окне кнопку "OK" и начните подписание сначала.

Также может появиться сообщение, что приложение уже запущено. В этом случае выключите другой экземпляр приложения, запущенный на данном компьютере.

6. Выберите ключ.

   Если необходимо подписать все выбранные документы одним и тем же ключом, установите отметку в поле "Запомнить ключ и пароль".

7. Нажмите кнопку "Подписать".

   На экране появится запрос на ввод пароля или PIN-кода.

8. Введите пароль или PIN-код и нажмите кнопку "OK".

   Если была установлена отметка "Запомнить ключ и пароль", все выбранные документы будут подписаны. Если отметка не была установлена, для подписания каждого документа потребуется выбирать ключ и вводить пароль или PIN-код.

Приложение

Восстановление ключа

Возникновение нештатной ситуации, например, отключение питания или извлечение ключевого носителя во время подписания документов, может привести к сбою, в результате которого ключ подписания, хранящийся на USB-флеш-накопителе, становится недоступным. В этом случае для восстановления утраченного ключа выполните следующее:

1. Вставьте ключевой накопитель с утраченным ключом и с помощью файлового менеджера откройте его содержимое.
2. Найдите файл **<file name>.p15.new_0~**, где <file name> – наименование утраченного ключа, и переименуйте его в **<file name>.p15**.
3. Найдите файл **<file name>.p15.old_0~**, если он присутствует на ключевом носителе, и удалите его.

   Утраченный ключ будет восстановлен.

Примечание. Для восстановления ключа, сгенерированного средствами "КриптоПро CSP", выполните аналогичные действия над парой файлов **<path name>/primary.key** и **<path name>/masks.key**. Также можно использовать специальное программное обеспечение от компании "Крипто-Про".

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.