#### **Руководство по генерации ключей и выпуску сертификата электронной подписи пользователя для подсистемы «Прямая интеграция»**

1. **Установка клиентского модуля КриптоПро CSP**

Для работы с сертификатами электронной подписи в Подсистеме дистанционного банковского обслуживания «Прямая интеграция» на клиентской стороне необходимо установить программное обеспечение КриптоПро (CryptoPro) CSP **версии не ниже 4.х.** Данное ПО приобретается клиентом самостоятельно (информацию о актуальной версии ПО можно узнать на сайте разработчика по адресу <https://www.cryptopro.ru/products/csp_5_0> ). В случае наличия указанного ПО на клиентской стороне, необходимо перейти к разделу 2 настоящего Руководства по генерации ключей и выпуску сертификата электронной подписи пользователя.

* 1. Запустить мастер установки КриптоПро CSP – CSPSetup.exe.



* 1. Нажать кнопку «Установить».



* 1. Дождаться окончания установки.



* 1. Нажать кнопку «ОК».

Внимание! Для работы с криптотокенами JaCarta 2 ГОСТ необходимо использовать КриптоПро CSP с версией продукта 4.0.9963:



1. **Генерация запроса на сертификат электронной подписи пользователя на клиентской стороне**

**!Важно!**

Перед генерацией запроса на сертификат проверьте, что в настройках операционной системы в языке программ, не поддерживающих Юникод, установлен текущий язык «Русский (Россия)».



Генерация ключей и выпуск сертификатов электронной подписи пользователей клиента производится на отдельной странице по ссылке <https://www.bankline.ru/servlets/ibc-new?pagename=GenCert>

В целях тестирования работоспособности взаимодействия клиента и банка с использованием Подсистемы дистанционного банковского обслуживания «Прямая интеграция» пользователи могут воспользоваться тестовым стендом Подсистемы и сгенерировать тестовый сертификат по ссылке: <https://www6.bankline.ru/servlets/ibc-test-new?pagename=GenCert>

Последовательность действий:

* 1. Убедиться, что установлен плагин для работы с уже установленной CryptoPRO CSP. При необходимости, скачать и запустить инсталлятор плагина RequCertPlugin



Проверить, установлен ли у вас плагин RequCertPlugin и текущую версию плагина можно, запустив Панель управления -> Программы и компоненты:



* 1. Ввести полученные от сотрудников банка данные: Код клиента (например, 1234567890), Код пользователя (например, 1234567890iii) и ФИО пользователя (например, Иванов Иван Иванович) и нажать кнопку «Войти». ВАЖНО: Код клиента и Код пользователя необходимо получить у сотрудника Банка. При этом вводимые данные «чувствительны» к регистру.



* 1. Проверить правильность заполненных данных по клиенту.

При использовании файлового обмена (каналы FTPs, Транзит 2.0) в поле «Тип сертификата» строго должно быть выбрано значение «Для подписи и шифрования».

В случае корректного заполнения – нажать кнопку «Сгенерировать запрос». В случае заполнения некорректными данными – необходимо нажать кнопку «Назад» и обратиться к сотруднику банка.



* 1. В отобразившемся окне «Генерация ключа» необходимо оставить значение «ГОСТ Криптопровайдер» и нажать кнопку «ОК».



* 1. В запустившемся окне CryptoPro CSP выберите тип носителя (реестр, локальный/съемный диск/криптотокен) и нажмите «ОК».



* 1. Начнется техническая процедура создания криптографических ключей– двигайте мышкой, нажимайте кнопки на клавиатуре, пока отображается индикатор.



* 1. По завершении генерации ключей будет запрошен пароль к контейнеру с ключом – придумайте, запомните и введите его 2 раза:



* 1. Ключи будут сохранены на носителе, а в Личном кабинете отобразится следующая страница:



* 1. Ваш запрос направлен в банк – необходим выпуск сертификата в Удостоверяющем Центре банка. Нажмите «Вернуться на страницу генерации запроса на сертификат».
	2. Запрос будет отображаться на экране справа в разделе «Запросы на сертификат».



* 1. Необходимо проинформировать контактное лицо банка о завершении процедуры запроса сертификата пользователя - сотрудники банка выпустят сертификат пользователя и сообщат вам об этом.
1. **Установка и печать сертификата пользователя на клиентской стороне**

После получения информации из банка о том, что сертификат выпущен, необходимо установить сертификат на клиентской стороне.

Для этого необходимо войти на страницу сервиса (для генерации рабочего сертификата <https://www.bankline.ru/servlets/ibc-new?pagename=GenCert>; для генерации тестового сертификата <https://www6.bankline.ru/servlets/ibc-test-new?pagename=GenCert>) – аналогично п.2.1. настоящей инструкции.

* 1. В разделе «Запросы на сертификат» необходимо выбрать сертификат и нажать кнопку «Установить».



* 1. Отобразится окно ввода пароля к контейнеру с ключом:



* 1. Введите пароль к контейнеру, использованный в п.2.7

Важно! По согласованию с вашей службой безопасности возможно сохранить введенный пароль и больше не вводить его – для этого необходимо отметить галку «Сохранить пароль».

* 1. Нажмите «ОК» и появится окно с подтверждением, что сертификат установлен:



* 1. В случае работы в Internet Explorer: если окно подтверждения установки не появилось, значит, браузер блокирует установку сертификата. Для разрешения установки перейдите, находясь на странице Личного кабинета, в настройки безопасности браузера (Свойства браузера-> Безопасность), добавьте адрес сайта в Надежные (кликнуть на эмблему зеленой галочки, нажать кнопку «Сайты», нажать кнопку «Добавить»). Затем необходимо передвинуть указатель уровня безопасности для Надежных сайтов на «Низкий», нажать «ОК» и перезапустить браузер.

Внимание! После установки сертификата не забудьте вернуть уровень безопасности Надежных сайтов на тот, который был установлен до выполнения данного пункта инструкции.

* 1. Нажмите «Понятно».

После установки необходимо выбрать сертификат – появится кнопка «Печать Акта».

Система формирует Акт автоматически. Необходимо выгрузить Акт о признании (автоматически выгружается 2 (два) экземпляра акта), подписать его и предоставить сотруднику банка.

Акт может быть подписан в электронном виде с использованием канала связи, позволяющего использовать усиленную квалифицированную электронную подпись, (например, система ЭДО Контур Диадок).

После подтверждения сертификата сотрудником банка, сертификат получит статус «Подтвержден», что означает готовность сертификата к использованию.



1. **Установка сертификатов банка и УЦ на клиентской стороне**
	1. Для завершения настройки клиентского места необходимо установить сертификаты банка, удостоверяющего центра и список отзывов сертификатов на компьютере пользователя клиента, с которого предполагается осуществлять взаимодействие с банком. Указанные сертификаты, содержащие открытые ключи банка и УЦ, и список отзывов в виде отдельных файлов, размещены на сайте банка (для продуктивной среды по ссылке - <https://api.rosbank.ru/doc/sertifikaty-prod.zip/d>, а для тестовой среды по ссылке - <https://api.rosbank.ru/doc/sertifikaty-test.zip/d>).
	2. Установить сертификат УЦ (certCA\_2012\_256.cer) в хранилище «Доверенные корневые центры сертификата». Для этого в браузере Microsoft Edge открыть «Настройки и прочее → Настройки → Конфиденциальность, поиск и службы → Безопасность → Управление сертификатами -> Доверенные корневые центры сертификации». С помощью кнопки «Импорт…» добавить сертификат (либо просто кликнуть по файлу сертификата и нажать «Установить»). Убедиться, что сертификат УЦ отображается на закладке «Доверенные корневые центры сертификации».
	3. Установить сертификат банка (cert\_h2h\_rb\_ib.cer). Для этого в браузере Microsoft Edge открыть «Настройки и прочее → Настройки → Конфиденциальность, поиск и службы → Безопасность → Управление сертификатами -> Доверенные корневые центры сертификации». С помощью кнопки «Импорт…» добавить сертификат (либо просто кликнуть по файлу сертификата и нажать «Установить»). Убедиться, что сертификат Банка отображается на закладке «Другие пользователи».
	4. Установить полученный из банка список отзывов (для продуктивной среды 01032019\_2012256.crl, для тестовой среды - crl2012256.crl). Для этого кликнуть на файле правой кнопкой мыши и выбрать «Установить список отзывов (CRL)».
	5. Проверьте готовность сертификата пользователя к работе:

- откройте свойства сертификата пользователя, на вкладке «Общие» присутствует фраза: «Есть закрытый ключ для этого сертификата».



- на вкладке «Путь сертификации» нет предупреждений об отсутствии сертификатов.



После выполнения всех указанных выше действий сертификат банка и УЦ на клиентской стороне установлен, все установленные сертификаты готовы к использованию.

1. **Добавление новой организации в холдинг**

Выпущенный сертификат связан с организацией, код которой использовался для входа в данный Личный кабинет. Но его можно настроить для подписания документов других организаций. Для этого необходимо в списке «Запросов на сертификаты» выделить нужный сертификат галкой и нажать кнопку «Добавить организацию».



В появившемся окне необходимо ввести код клиента, который включается в холдинг (клиент, который предоставит данному пользователю полномочия подписания документов от своего имени в соответствии с назначенным уровнем подписи), и нажать «Напечатать акт».



Система формирует Акт автоматически. В каждом из двух экземпляров сформированного акта необходимо заполнить наименование клиента (не заполняется автоматически), подписать его и предоставить сотруднику банка для предоставления данному пользователю полномочий подписывать документы от добавленной организации.

Акт может быть подписан в электронном виде с использованием канала связи, позволяющего использовать усиленную квалифицированную электронную подпись, (например, система ЭДО Контур Диадок).