ОБЪЕДИНЁННОЕ
КРЕДИТНОЕ
БЮРО

РЕГЛАМЕНТ
обмена электронными документами между ЗАО «ОКБ» и Клиентом («Регламент»)

Версия №4 от 25.03.2015 г.

1. Общие положения

1.1. Настоящий Регламент определяет порядок обмена электронными документами, подписанными электронной подписью, между ЗАО «ОКБ» (далее – «Бюро») и Клиентом в рамках Соглашения об обмене электронными документами (далее – «Соглашение») между ЗАО «ОКБ» и Клиентом.

1.2. Термины и определения

Термины, перечисленные в Федеральном законе от 06.04.2011 №63-ФЗ «Об электронной подписи», применяются в настоящем Регламенте в соответствии с определениями, данными в указанном законе.

Клиент Бюро или Клиент – юридическое лицо или индивидуальный предприниматель, взаимодействующий с Бюро в рамках договоров по оказанию Бюро услуг данному юридическому лицу или индивидуальному предпринимателю.

Оператор Удостоверяющего Центра или Оператор УЦ – юридическое лицо, заключившее с Удостоверяющим Центром договор на предоставление услуг по изготовлению сертификатов ключей подписей и уполномоченное Удостоверяющим Центром осуществлять регистрацию пользователей, изготовление и управление сертификатами ключей подписей Пользователей Удостоверяющего Центра.

Пользователь Удостоверяющего Центра – физическое лицо, зарегистрированное в Удостоверяющем Центре и являющееся полномочным представителем Стороны.

Регламенты Удостоверяющего Центра – документы, описывающие порядок взаимодействия Пользователей УЦ, Оператора УЦ и Удостоверяющего Центра в процессе создания, выдачи и использования сертификатов ключей проверки электронной подписи. Регламенты Удостоверяющего Центра ООО «КРИПТО-ПРО» доступны на сайте ООО «КРИПТО-ПРО» по адресу http://cpca.cryptopro.ru.

Соглашение – соглашение об обмене электронными документами, заключенное между Сторонами.

Средство криптографической защиты информации или СКЗИ – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В документообороте между Сторонами используется сертифицированные СКЗИ производства ООО «КРИПТО-ПРО», в частности, программное обеспечение КриптоПРО CSP.**Стороны** – совместное наименование Клиента и Бюро при взаимодействии в рамках договоров между ними. При этом Клиент и Бюро отдельно также именуются **Сторона**.

Удостоверяющий Центр или УЦ – Общество с ограниченной ответственностью «КРИПТО-ПРО» (ОГРН 1037700085444, ИНН/КПП 7717107991/771901001, адрес регистрации 105318, Москва г, Ибрагимова ул., дом 31, офис 30Б).

Электронная подпись или ЭП - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. При обмене электронными документами в рамках любого соглашения Сторонами используется в качестве электронной подписи усиленная неквалифицированная электронная подпись («УНЭП»). В любом соглашении, договоре или ином документе между Сторонами под термином «электронная подпись», «ЭП», «электронно-цифровая подпись», «электронная цифровая подпись» или «ЭЦП» подразумевается УНЭП.

2. Порядок подключения к системе обмена электронными документами.

2.1. Подключение Клиента к системе обмена электронными документами осуществляется после заключения Сторонами Соглашения.

2.2. Клиент предоставляет в Бюро:

- файлы сертификатов ключей проверки Электронной подписи уполномоченных лиц Клиента, которые будут использоваться для простановки ЭП и шифрования при обмене электронными документами в рамках Соглашения, а также оформленные распечатки указанных сертификатов (форма приведена в

Приложении №3 к настоящему Регламенту) и письмо о регистрации данных сертификатов в информационной системе Бюро (форма приведена в Приложении №1 к настоящему Регламенту);

- доверенности Клиента на должностных лиц Клиента, которые уполномочены подписывать электронные документы Электронной подписью. Доверенности могут быть оформлены по форме, приведенной в Приложении №2 к настоящему Регламенту, либо по форме доверенности Пользователя Удостоверяющего Центра, приведенной в приложениях к Регламентам Удостоверяющего Центра;

- копию приказа о назначении администратора абонентского пункта, отвечающего за действия, осуществляемые от лица Клиента на данном абонентском пункте, и администратора информационной безопасности, отвечающего за обеспечение защиты информации на данном абонентском пункте.

2.3. Клиент организует абонентский пункт системы обмена электронными документами, который должен удовлетворять требованиям, указанным в эксплуатационных документах на СКЗИ по обеспечению условий функционирования и безопасности. О готовности к работе Клиент составляет в 2-х экземплярах Акт готовности к работе в системе обмена электронными документами (форма Акта приведена в Приложении №4 к Регламенту), подписываемый руководителями подразделений, отвечающих за автоматизацию и за обеспечение безопасности, и утверждаемый руководством Клиента. Один экземпляр Акта готовности, подписанный со стороны Клиента, высылается в Бюро.

3. Требования по обеспечению безопасности функционирования абонентского пункта

3.1. Абонентский пункт размещается в охраняемом помещении, оборудованном системой охранной сигнализации, исключающей доступ в помещение посторонних лиц.

3.2. Дискеты и другие носители с криптографическими ключами должны храниться в металлических шкафах (сейфах), исключающих несанкционированный доступ к ним посторонних лиц.

3.3. Системные блоки компьютеров абонентского пункта должны быть оборудованы средствами защиты от несанкционированного вскрытия.

3.4. Криптографические ключи и их носители должны быть учтены в выделенных для этих целей журналах.

3.5. Рекомендуется изготовление одного дубликата носителя с криптографическими ключами, предназначенного для использования в случае физического выхода из строя основного носителя.

4. Взаимодействие Сторон

4.1. Для обмена информацией с Бюро Клиентом создаются ключи Электронной подписи и самостоятельно получаются в Удостоверяющем центре (напрямую, либо через Оператора Удостоверяющего центра) сертификаты ключей проверки Электронной подписи для ответственных лиц, которые будут подписывать Электронной подписью электронные документы при обмене информацией в рамках Соглашения.

4.2. Информация предоставляется в Бюро в виде электронного документа, формат которого устанавливается Бюро.

5. Сроки действия ключа Электронной подписи и сертификата ключа проверки Электронной подписи

5.1. Срок действия ключа подписи составляет 1 (один) год.

5.2. Срок действия сертификата ключа проверки Электронной подписи составляет 5 (пять) лет, что отражается в параметрах сертификата. Не позже, чем за 15 (пятнадцать) дней до истечения срока действия сертификата Сторона, у которой срок действия сертификата истекает, должна заново пройти процедуру формирования криптографических ключей и получения сертификата в соответствии с п.4.1 настоящего Регламента. При вступлении в действие нового сертификата прежний сертификат считается

отмененным. Вновь выпущенный сертификат передается другой Стороне в порядке, определенном в п. 2.2 настоящего Регламента.

5.3. Каждая Сторона вправе отменить действие сертификата своего уполномоченного лица, передав другой Стороне письменное уведомление об отмене действия сертификата в виде официального письма с указанием владельца данного сертификата, серийного номера данного сертификата, даты и времени, с которых данный сертификат считается отмененным, а также причины отмены данного сертификата.

5.4. Ключ проверки Электронной подписи Пользователя Удостоверяющего Центра Стороны считается отмененным с даты отмены действия ключа, указанной в уведомлении об отмене действия сертификата, но не ранее даты получения и регистрации в журнале входящей корреспонденции этого уведомления другой Стороной.

6. Действия при компрометации ключа Электронной подписи

6.1. При компрометации ключа Электронной подписи любой из Сторон такая Сторона должна немедленно приостановить обмен электронными документами, а также поставить в известность другую Сторону письменным уведомлением об отмене действия соответствующего сертификата ключа проверки Электронной подписи в соответствии с п.5.3 настоящего Регламента.

6.2. Для выявления причины компрометации ключа Электронной подписи Клиента у Клиента создается комиссия по расследованию данного инцидента. Результаты работы комиссии оформляются заключением. Один экземпляр заключения направляется в Бюро.

6.3. Скомпрометированные ключи Электронной подписи подлежат замене.

7. Список отозванных сертификатов

7.1. Для проверки действительности сертификата (сертификат не отозван) используется список отозванных сертификатов (СОС), который должен регулярно обновляться на всех рабочих местах Сторон.

7.2. Ответственность за поддержание СОС в актуальном состоянии на рабочих местах Сторон каждая Сторона несет самостоятельно.

8. Разрешение споров

8.1. Все споры и разногласия, возникающие в связи с толкованием и/или применением Регламента, разрешаются путем переговоров после предъявления претензии в письменном виде другой Стороне.

8.2. При недостижении согласия по истечении 30 (Тридцати) календарных дней с момента письменного предъявления претензии любая из Сторон имеет право передать спор на рассмотрение в Арбитражный суд города Москвы.

Приложение № 1 к Регламенту обмена электронными документами между ЗАО «ОКБ» и Клиентом
(Письмо о регистрации сертификатов Пользователей)

Генеральному директору
ЗАО «ОКБ»

Зеленскому Д.В.

Исх. №_____

от «_____» _____ 20___ г.

Уважаемый Даниэль Викторович!

Просим при взаимодействии между <Наименование Клиента> и ЗАО «ОКБ» использовать следующие сертификаты доверенных лиц:

– <Фамилия Имя Отчество Пользователя> (сертификат № <серийный номер сертификата>)

– <Фамилия Имя Отчество Пользователя> (сертификат № <серийный номер сертификата>)

– <Фамилия Имя Отчество Пользователя> (сертификат № <серийный номер сертификата>)

Доверенности на указанных лиц и бланки указанных сертификатов прилагаются.

Приложение: по тексту на ___ листах

Подпись уполномоченного лица организации, дата подписания заявления

Печать организации

Приложение № 2 к Регламенту обмена электронными документами между ЗАО «ОКБ» и Клиентом
(Форма доверенности Пользователя Удостоверяющего центра)

Доверенность

г. _____ «___» _____20___ г.

_____
(полное наименование организации, включая организационно-правовую форму)

в лице _____,
(должность)
_____,
(фамилия, имя, отчество)

действующего на основании _____

уполномочивает _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

от имени _____
(наименование организации)

выступать в роли Пользователя Удостоверяющего центра ООО «КРИПТО-ПРО» и осуществлять действия в рамках Регламента обмена электронными документами между ЗАО «ОКБ» и Клиентом.

Представитель наделяется правом расписываться в соответствующих документах для исполнения поручений, определенных настоящей Доверенностью.

Настоящая доверенность действительна по «____» _____ 20____ г. включительно.

Подпись уполномоченного представителя Фамилия И.О. _____ подтверждаю.

Должность и Фамилия И.О. уполномоченного лица организации

Подпись уполномоченного лица организации, дата подписания заявления

Печать организации

Приложение № 3 к Регламенту обмена электронными документами между ЗАО «ОКБ» и Клиентом
(Пример Бланка сертификата Пользователя Удостоверяющего центра; внешний вид и оформление конечных документов могут отличаться)

Удостоверяющий Центр КРИПТО-ПРО
Бланк сертификата открытого ключа

Сведения о сертификате:
Этот сертификат:
Подтверждает удаленному компьютеру идентификацию вашего компьютера
Защищает сообщения электронной почты
Обеспечивает идентификацию пользователя на центре регистрации
Кому выдан:
Иванов Иван Иванович
Кем выдан:
УЦ КРИПТО-ПРО
Действителен с 30 марта 2006 г. 13:48:00 UTC по 30 апреля 2006 г. 13:58:00 UTC
Версия: 3 (0x2)
Серийный номер: 1A97 6D3E 0004 0000 098B
Издатель сертификата: CN = УЦ КРИПТО-ПРО, O = ООО КРИПТО-ПРО, L = Москва, C = RU, E = cpca@cryptopro.ru
Срок действия:
Действителен с: 30 марта 2006 г. 13:48:00 UTC
Действителен по: 30 апреля 2006 г. 13:58:00 UTC
Владелец сертификата: CN = Иванов Иван Иванович, OU = Кредитный отдел, O = Ваш Банк (ОАО), L = Москва, C = RU, E = iv@vb.ru
Открытый ключ:
Алгоритм открытого ключа:
Название: ГОСТ Р 34.10-2001
Идентификатор: 1.2.643.2.2.19
Параметры: 30 12 06 07 2a 85 03 02 02 24 00 06 07 2a 85 03 02 02 1e 01
Значение: 0440 E356 2D4F F523 CA3F 76F0 4001 6137 1944 356D F1B9 E281 1AC9 BA84 07AC 5094 0F1E 4A6C E390 3E03 08C6 6A87 E2B4 C672 4342 A07D F35E 153C B149 1DED 40EE 5756 AD41
Расширения сертификата X.509
1. Расширение 2.5.29.15 (критическое)
Название: Использование ключа
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)
2. Расширение 2.5.29.37
Название: Улучшенный ключ
Значение: Защищенная электронная почта (1.3.6.1.5.5.7.3.4) Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
Название: Идентификатор ключа субъекта
Значение: ef a7 07 eb 85 78 c0 83 13 1d 16 76 33 f4 32 cb 85 94 b8 0a
4. Расширение 2.5.29.35
Название: Идентификатор ключа центра сертификатов
Значение: Идентификатор ключа=ca b8 26 2e 1f 73 39 30 d0 35 58 f1 4e 3c 63 f2 37 c4 a1 4a
5. Расширение 2.5.29.31
Название: Точки распространения списков отзыва (CRL)
Значение: [1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя:
URL=http://cpca.cryptopro.ru/RA/CDP/cab8262e1f733930d03558f14e3c63f237c4a14a.crl
Подпись Удостоверяющего центра:
Алгоритм подписи:
Название: ГОСТ Р 34.11/34.10-2001
Идентификатор: 1.2.643.2.2.3
Параметры: 05 00
Значение: 2C0E C386 2FF6 6C6F E665 7CDA 2506 9D24 BCD8 5312 9E12 5225 A854 AD5F C3FB 03DB C0FF 12F5 74F1 13D4 78B8 AE28 2CA0 F116 AD43 D88A F4A3 B676 00BD 1123 5E1A 1F76

Подпись владельца сертификата: _____/_____

"___" _____ 20__ г.

Должность и Ф.И.О. уполномоченного лица организации
Подпись уполномоченного лица организации, дата подписания заявления
Печать организации

Приложение № 4 к Регламенту обмена электронными документами между ЗАО «ОКБ» и Клиентом

УТВЕРЖДАЮ

_____

(должность)

_____ _____

(подпись) (Фамилия И.О.)

" " _____ г.

АКТ

готовности

_____

(наименование Клиента)

к работе в системе обмена электронными документами между ЗАО «ОКБ» и Клиентом – участником формирования отчетов и запросов по кредитным историям.

Во исполнение Приказа №____от _____ специалистами _____ проведена проверка готовности к работе абонентского пункта (АРМ) системы обмена электронными документами между ЗАО «ОКБ» и Клиентом.

УСТАНОВЛЕНО:

1. Размещение и техническое состояние аппаратных средств абонентского пункта и состояние программного обеспечения соответствуют предъявляемым требованиям.
2. Ответственные должностные лица назначены Приказом №___ от _____
3. Информационная безопасность абонентского пункта обеспечивается следующими защитными мерами и средствами:

- помещение оборудовано охранной сигнализацией, средствами контроля, управления и регистрации физического доступа персонала в помещения;
- все транспортные файлы, содержащие электронные документы, исполняются только с Электронной подписью и при передаче через телекоммуникационную сеть шифруются;
- ключи Электронной подписи Клиента и Бюро зарегистрированы и введены в действие установленным порядком. Ключевые носители с криптографическими ключами хранятся и используются в соответствии с требованиями эксплуатационной документации.
- в системе разграничения доступа к программным и информационным ресурсам абонентского пункта используются только персональные (личные) пароли, изменяемые не реже одного раза в 6 (шесть) месяцев;

ВЫВОД: Абонентский пункт готов к работе по обмену электронными документами в системе обмена электронными документами между ЗАО «ОКБ» и Клиентом.

Настоящий Акт составлен на ____ страницах в двух экземплярах, имеющих одинаковую юридическую силу.

_____

Должность Ф.И.О. подпись

_____

Должность Ф.И.О. подпись