# Регламент предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО" (приложение к соглашению об электронном документообороте в рамках договора об оказании информационных услуг (предоставлении кредитных отчетов))

### Приложение к Соглашению об электронном документообороте

### РЕГЛАМЕНТ предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО"

### 1. Сведения об Операторе Удостоверяющего центра

Открытое акционерное общество "Национальное бюро кредитных историй", именуемое в дельнейшем "Оператор Удостоверяющего центра" ("Оператор"), зарегистрировано на территории Российской Федерации. Свидетельство о государственной регистрации и внесении записи в ЕГРЮЛ за основным государственным регистрационным номером 1057746710713.

Реквизиты ОАО "НБКИ".

Полное наименование: Открытое акционерное общество "Национальное бюро кредитных историй"

Юридический адрес: 121069, г. Москва, Скатертный пер., д. 20, стр. 1

Фактический адрес: 125009, г. Москва, ул. Б. Никитская, д. 24/1, стр. 5

Адрес для корреспонденции: 121069, г. Москва, Скатертный пер., д. 20, стр. 1

Банковские реквизиты (наименование банка, БИК, р/с, к/с):

- Краснопресненское отделение Сбербанка РФ N 1569/01664

- БИК 044525225

- р/с 40702810538170107483

- к/с 30101810400000000225

ИНН/КПП: 7703548386/770301001

ОГРН: 1057746710713

ОКВЭД: 72.4

ОКПО: 77294012

Контактные телефоны, факс, адрес электронной почты:

- тел./факс: (495) 221-78-37; e-mail: support@nbki.ru.

### 2. Сведения об Удостоверяющем центре

Удостоверяющим центром, обеспечивающим согласно законодательству Российской Федерации изготовление сертификатов ключей подписей, является Общество с ограниченной ответственностью "КРИПТО-ПРО".

ООО "КРИПТО-ПРО" в качестве профессионального участника рынка услуг по изготовлению и выдаче сертификатов ключей подписей осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий.

1. Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление распространения шифровальных (криптографических) средств.

2. Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств.

3. Лицензия Центра ФСБ России по лицензированию, сертификации и защите государственной тайны от 30 ноября 2008 г. N 6389У на право предоставления услуг в области шифрования информации.

4. Лицензия ФСТЭК России от 2 февраля 2006 г. 0439 на деятельность по технической защите конфиденциальной информации.

Сертификаты ключей подписей уполномоченного лица Удостоверяющего центра зарегистрированы Уполномоченным федеральным органом исполнительной власти Российской Федерации в части применения ЭЦП в Едином государственном реестре сертификатов уполномоченных лиц удостоверяющих центров.

### 3. Термины и определения

Электронный документ - документ, информация в котором представлена в электронно-цифровой форме.

Средство электронной цифровой подписи - средство криптографической защиты информации (СКЗИ) "КРИПТО-ПРО CSP", обеспечивающее реализацию следующих функций - создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей.

Электронная цифровая подпись (ЭЦП) - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата открытого ключа подписи и предназначенная для создания в электронных документах ЭЦП с использованием средств электронной цифровой подписи.

Закрытый ключ ЭЦП действует на определенный момент времени (действующий закрытый ключ), если:

наступил момент времени начала действия закрытого ключа;

срок действия закрытого ключа не истек;

сертификат открытого ключа подписи, соответствующий данному закрытому ключу, не аннулирован (не отозван) и действие его не приостановлено.

Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу ЭЦП, предназначенная для подтверждения с использованием средств ЭЦП подлинности ЭЦП в электронном документе.

Сертификат открытого ключа подписи (сертификат открытого ключа, сертификат ключа подписи) - электронный документ с ЭЦП уполномоченного лица Удостоверяющего центра, структура которого определяется настоящим Регламентом и который изготавливается Удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации владельца сертификата ключа подписи.

Сертификат открытого ключа подписи действует на определенный момент времени (действующий сертификат), если:

наступил момент времени начала действия сертификата открытого ключа;

срок действия сертификата открытого ключа не истек; сертификат открытого ключа не аннулирован (не отозван) и действие его не приостановлено.

Копия сертификата ключа подписи - документ на бумажном носителе, содержащий информацию из сертификата ключа подписи и заверенный собственноручной подписью ответственного лица Оператора Удостоверяющего центра и печатью Оператора Удостоверяющего центра.

Список отозванных сертификатов (СОС) - электронный документ с электронной цифровой подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Владелец сертификата ключа подписи - физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).

Псевдоним владельца сертификата ключа подписи - вымышленное имя физического лица, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Удостоверяющий центр - ООО "КРИПТО-ПРО", осуществляющее выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом "Об электронной цифровой подписи".

Оператор Удостоверяющего центра (Оператор) - Открытое акционерное общество "Национальное бюро кредитных историй", наделенное Удостоверяющим центром полномочиями по осуществлению действий по регистрации и управлению сертификатами ключей подписи Пользователей Удостоверяющего центра - полномочных представителей Стороны, присоединившейся к Регламенту.

Реестр Удостоверяющего центра - набор документов Удостоверяющего центра в электронной и (или) бумажной форме, включающий следующую информацию:

реестр заявлений на регистрацию в Удостоверяющем центре;

реестр зарегистрированных пользователей Удостоверяющего центра;

реестр заявлений на изготовление сертификата ключа подписи;

реестр заявлений на аннулирование (отзыв) сертификата ключа подписи;

реестр заявлений на приостановление/возобновление действия сертификата ключа подписи;

реестр заявлений на подтверждение подлинности ЭЦП в электронном документе;

реестр заявлений на подтверждение ЭЦП уполномоченного лица Удостоверяющего центра в изданных сертификатах; реестр сертификатов ключей подписи; реестр изготовленных списков отозванных сертификатов.

Уполномоченное лицо Удостоверяющего центра - физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов открытого ключа подписи и списков отозванных сертификатов.

Пользователь Удостоверяющего центра (Пользователь УЦ) - физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся полномочным представителем Стороны, присоединившейся к Регламенту.

Информационная система - корпоративная информационная система, устроителем которой является организатор системы, в которой используются закрытые ключи и сертификаты открытых ключей ЭЦП и предоставляются определенные услуги участникам этой системы.

Рабочий день Оператора Удостоверяющего центра (далее - рабочий день) - промежуток времени с 10.00 по 18.00 (время московское) каждого дня недели, за исключением выходных и праздничных дней.

Служба актуальных статусов сертификатов - сервис Удостоверяющего центра, обеспечивающий информирование пользователей о статусе сертификатов ключей подписей по протоколу OCSP (Online Certificate Status Protocol).

Служба штампов времени - сервис Удостоверяющего центра, обеспечивающий предоставление Пользователям Удостоверяющего центра штампов времени по протоколу TSP (Time-Stamp Protocol).

Список отозванных сертификатов (СОС) - электронный документ с ЭЦП уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было приостановлено.

Штамп времени электронного документа (штамп времени) - электронный документ, подписанный ЭЦП и устанавливающий существование определенного электронного документа на момент времени, указанный в штампе.

Cryptographic Message Syntax (CMS) - стандарт криптографических сообщений, описанный в RFC 3852 и RFC 3369. Удостоверяющий центр использует в своей работе криптографические сообщения, соответствующие данному стандарту с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)".

Online Certificate Status Protocol (OCSP) - протокол установления статуса сертификата открытого ключа, реализующий RFC 2560 "X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol - OCSP".

Public Key Cryptography Standarts (PKCS) - стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляют свою работу в соответствии со следующим стандартом PKCS - PKCS#10 - стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

Time-Stamp Protocol (TSP) - протокол получения штампа времени, реализующий RFC 3161 "Internet X.509 Public Key Infrastructure TimeStamp Protocol (TSP)".

### 4. Общие положения

4.1. Статус Регламента.

4.1.1. Настоящий Регламент предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО" (далее - Регламент) является договором присоединения в соответствии со статьей 428 Гражданского кодекса Российской Федерации.

4.1.2. Сторонами Регламента (далее - Стороны) являются Открытое акционерное общество "Национальное бюро кредитных историй", выступающее Оператором Удостоверяющего центра, и Сторона, присоединившаяся к Регламенту.

4.1.3. Любое заинтересованное лицо может ознакомиться с Регламентом в офисе Оператора Удостоверяющего центра по адресу: 125009, г. Москва, ул. Б. Никитская, д. 24/1, стр. 5.

4.2. Присоединение к Регламенту.

4.2.1. Присоединение к Регламенту осуществляется путем подписания и предоставления Оператору Удостоверяющего центра Подписного листа к Регламенту по форме Приложения 1 настоящего Регламента.

4.2.2. Факт присоединения лица к Регламенту является полным принятием условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания Подписного листа.

4.2.3. После присоединения к Регламенту в установленном порядке Стороны вступают в соответствующие договорные отношения на неопределенный срок.

4.2.4. Каждая из Сторон вправе без обращения в суд расторгнуть настоящий Регламент, письменно уведомив другую сторону за 30 календарных дней до дня расторжения. При этом Стороны в течение срока предупреждения до дня прекращения действия Регламента обязаны разрешить между собой все денежные и иные имущественные вопросы, связанные с настоящим Регламентом.

4.2.5. Прекращение действия Регламента не освобождает Стороны от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и от ответственности за его неисполнение (ненадлежащее исполнение).

4.3. Применение Регламента.

4.3.1. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

4.3.2. В случае противоречия и (или) расхождения названия какого-либо раздела Регламента со смыслом какого-либо пункта, в нем содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

4.3.3. В случае противоречия и (или) расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента Стороны считают доминирующими смысл и формулировки Регламента.

4.4. Изменение (дополнение) Регламента.

4.4.1. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.

4.4.2. Уведомление присоединившейся Стороны о внесении изменений (дополнений) в Регламент осуществляется Оператором направлением по электронной почте в адрес уполномоченного представителя присоединившейся Стороны - Пользователя Удостоверяющего центра - соответствующего информационного сообщения.

4.4.3. Все изменения (дополнения), вносимые Оператором в Регламент по собственной инициативе и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для присоединившейся Стороны по истечении календарных суток с даты уведомления присоединившейся Стороны о внесении указанных изменений (дополнений).

4.4.4. Все изменения (дополнения), вносимые Оператором в Регламент в связи с изменением действующего законодательства Российской Федерации, вступают в силу одновременно с вступлением в силу изменений (дополнений) в указанных актах.

4.4.5. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу. В случае несогласия с изменениями (дополнениями) Пользователь Удостоверяющего центра имеет право до вступления в силу таких изменений (дополнений) на расторжение Регламента в порядке, предусмотренном п. 4.2.4 настоящего Регламента.

4.4.6. Все приложения, изменения и дополнения к настоящему Регламенту являются его составной и неотъемлемой частью.

### 5. Предоставление информации

5.1. Оператор вправе запросить у Стороны, присоединившейся к Регламенту, а присоединившаяся Сторона обязана предоставить Оператору документы, подтверждающие следующую информацию:

5.1.1. Наименование Организации и основной государственный регистрационный номер, идентификационный номер налогоплательщика.

5.1.2. Нотариально заверенную копию Устава Организации; нотариально заверенную копию учредительного договора (если есть).

5.1.3. Нотариально заверенную копию свидетельства ИМНС о государственной регистрации.

5.1.4. Копии протоколов либо иных документов о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и (или) надлежащим образом оформленные доверенности.

5.1.5. Сведения, необходимые для идентификации полномочного представителя Стороны, присоединившейся к Регламенту: фамилия, имя, отчество, номер паспорта, дата и кем выдан, место регистрации.

### 6. Права и обязанности Сторон

6.1. Оператор обязан:

6.1.1. Предоставить Пользователю Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра.

6.1.2. Обеспечить регистрацию пользователей в Удостоверяющем центре по заявлениям на регистрацию в Удостоверяющем центре в соответствии с порядком, определенным в настоящем Регламенте.

6.1.3. Занести регистрационную информацию Пользователей Удостоверяющего центра в Реестр Удостоверяющего центра.

6.1.4. Обеспечить изготовление сертификата ключа подписи зарегистрированного в Удостоверяющем центре лица по заявлениям на изготовление сертификата ключа подписи в соответствии с порядком, определенным в настоящем Регламенте, и официально уведомить об этом владельца изготовленного сертификата ключа подписи.

6.1.5. В случае изготовления Оператором закрытого и открытого ключа пользователя Оператор обязан:

выполнять процедуру генерации ключей и их запись на сменный магнитный носитель только с использованием сертифицированного в соответствии с правилами сертификации Российской Федерации СКЗИ, поддерживаемого Удостоверяющим центром;

обеспечить сохранение в тайне изготовленного закрытого ключа пользователя.

6.1.6. Аннулировать (отозвать) сертификат ключа подписи Пользователя Удостоверяющего центра по заявлению на аннулирование (отзыв) сертификата ключа подписи в соответствии с порядком, определенным в настоящем Регламенте.

6.1.7. Приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра по заявлению на приостановление действия сертификата ключа подписи в соответствии с порядком, определенным в настоящем Регламенте.

6.1.8. Возобновить действие сертификата ключа подписи Пользователя Удостоверяющего центра по заявлению на возобновление действия сертификата ключа подписи (исключительно в случае поступления заявления в период срока, на который действие сертификата было приостановлено) в соответствии с порядком, определенным в настоящем Регламенте.

6.2. Сторона, присоединившаяся к Регламенту, обязана:

6.2.1. Известить Удостоверяющий центр об изменениях в наименовании Организации, государственного регистрационного номера, идентификационного номера налогоплательщика и по требованию Удостоверяющего центра предоставить подтверждающие документы в течение 5 рабочих дней с момента регистрации изменений.

6.2.2. Пользователь Удостоверяющего центра, являющийся полномочным представителем присоединившейся Стороны, обязан:

6.2.2.1. Сформировать открытые и закрытые ключи подписи на своем рабочем месте только с использованием средства ЭЦП и программного обеспечения, предоставляемого Удостоверяющим центром.

6.2.2.2. Хранить в тайне личный закрытый ключ, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования.

6.2.2.3. Применять для формирования ЭЦП только действующий личный закрытый ключ.

6.2.2.4. Не применять личный закрытый ключ, если ему стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.2.5. Применять личный закрытый ключ только в соответствии с областями использования, указанными в соответствующем данному закрытому ключу сертификате ключа подписи (поля Key Usage, Extended Key Usage сертификата ключа подписи).

6.2.2.6. Немедленно обратиться к Оператору с заявлением на приостановление действия сертификата ключа подписи в случае потери, раскрытия, искажения личного закрытого ключа, а также в случае если Пользователю Удостоверяющего центра стало известно, что этот ключ используется или использовался ранее другими лицами.

6.2.2.7. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на аннулирование (отзыв) которого подано на рассмотрение Оператором, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата по момент времени официального уведомления об аннулировании (отзыве) сертификата.

6.2.2.8. Не использовать личный закрытый ключ, связанный с сертификатом ключа подписи, заявление на приостановление действия которого подано на рассмотрение Оператором, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата по момент времени официального уведомления о приостановлении действия сертификата.

6.2.2.9. Не использовать личный закрытый ключ до предоставления Оператору подписанной копии сертификата ключа подписи, соответствующего данному закрытому ключу.

6.3. Оператор имеет право:

6.3.1. Отказать в регистрации в Удостоверяющем центре уполномоченному представителю Стороны, присоединившейся к Регламенту, в случае ненадлежащего оформления необходимых регистрационных документов.

6.3.2. Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на изготовление сертификата ключа подписи.

6.3.3. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на аннулирование (отзыв) сертификата ключа подписи.

6.3.4. Отказать в приостановлении/возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата ключа подписи.

6.3.5. Отказать в аннулировании (отзыве) сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.6. Отказать в приостановлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.7. Отказать в возобновлении действия сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если истек установленный срок действия закрытого ключа, соответствующего этому сертификату.

6.3.8. В одностороннем порядке приостановить действие сертификата ключа подписи Пользователя Удостоверяющего центра с обязательным уведомлением владельца сертификата ключа подписи, действие которого приостановлено, и указанием обоснованных причин.

6.3.9. Отказать в изготовлении сертификата ключа подписи Пользователя Удостоверяющего центра в случае, если использованное Пользователем Удостоверяющего центра для формирования запроса на сертификат ключа подписи СКЗИ не поддерживается Удостоверяющим центром.

6.4. Сторона, присоединившаяся к Регламенту, имеет право:

6.4.1. Получить сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

6.4.2. Получить список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром.

6.4.3. Применять сертификат ключа подписи уполномоченного лица Удостоверяющего центра для проверки ЭЦП уполномоченного лица Удостоверяющего центра в сертификатах ключей подписи, изготовленных Удостоверяющим центром.

6.4.4. Применять список отозванных сертификатов ключей подписи, изготовленный Удостоверяющим центром, для проверки статуса сертификатов ключей подписи, изготовленных Удостоверяющим центром.

6.4.5. Применять сертификат ключа подписи Пользователя Удостоверяющего центра для проверки ЭЦП электронных документов в соответствии со сведениями, указанными в сертификате ключа подписи.

6.4.6. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на регистрацию в электронном виде.

6.4.7. Воспользоваться предоставляемыми Удостоверяющим центром программными средствами для передачи по линиям связи в Удостоверяющий центр заявления на изготовление сертификата ключа подписи в электронном виде.

6.4.8. Воспользоваться предоставляемыми Удостоверяющим Центром программными средствами, чтобы получить и установить на свое рабочее место изготовленный Удостоверяющим центром сертификат ключа подписи.

6.4.9. Для хранения личного закрытого ключа применять любой носитель, поддерживаемый средством ЭЦП.

6.4.10. Обратиться к Оператору для аннулирования (отзыва) сертификата ключа подписи в течение срока действия соответствующего закрытого ключа.

6.4.11. Обратиться к Оператору для приостановления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа.

6.4.12. Обратиться к Оператору для возобновления действия сертификата ключа подписи в течение срока действия соответствующего закрытого ключа и срока, на который действие сертификата было приостановлено.

### 7. Ответственность Сторон

7.1. Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной Регламента своих обязательств.

7.2. Ответственность Сторон, не урегулированная положениями настоящего Регламента, регулируется законодательством Российской Федерации.

### 8. Разрешение споров

8.1. Сторонами в споре в случае его возникновения считаются Оператор и Сторона, присоединившаяся к Регламенту.

8.2. При рассмотрении спорных вопросов, связанных с настоящим Регламентом, Стороны будут руководствоваться действующим законодательством Российской Федерации.

8.3. Стороны будут принимать все необходимые меры к тому, чтобы в случае возникновения спорных вопросов решить их путем переговоров.

8.4. Спорные вопросы между Сторонами, неурегулированные путем переговоров, решаются в Арбитражном суде г. Москвы.

### 9. Порядок предоставления и пользования услугами Удостоверяющего центра

9.1. Регистрация Пользователей Оператором Удостоверяющего центра.

Оператор Удостоверяющего центра осуществляет регистрацию Пользователя в Удостоверяющем центре только в том случае, если Сторона, полномочным представителем которой является регистрирующееся лицо, присоединилась к настоящему Регламенту.

9.1.1. Регистрация пользователей и изготовление первого сертификата в централизованном режиме.

Регистрация Пользователя в Удостоверяющем центре осуществляется на основании заявления на регистрацию при личном прибытии лица, проходящего процедуру регистрации, в офис Оператора.

Форма заявления на регистрацию приведена в Приложении 3 к настоящему Регламенту.

Регистрирующееся лицо должно предоставить доверенность, выданную на его имя Стороной, присоединившейся к Регламенту, на совершение действий в рамках настоящего Регламента, по форме Приложения 4.

В случае если регистрирующееся лицо не может прибыть лично в офис Оператора, Сторона, присоединившаяся к Регламенту, должна выдать представителю, пребывающему в офис Оператора для регистрации, Доверенность на регистрацию соответствующего Пользователя. Форма Доверенности приведена в Приложении 5 к настоящему Регламенту.

Ответственный сотрудник Оператора Удостоверяющего центра выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту.

После положительной идентификации лица, проходящего процедуру регистрации, ответственный сотрудник Оператора Удостоверяющего центра принимает документы и осуществляет их рассмотрение.

Заявление на регистрацию рассматривается ответственным сотрудником Оператора Удостоверяющего центра в течение 1 (одного) часа с момента поступления.

В случае отказа в регистрации заявление на регистрацию вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника Оператора Удостоверяющего центра.

При принятии положительного решения ответственный сотрудник Оператора Удостоверяющего центра выполняет регистрационные действия по занесению регистрационной информации в реестр Удостоверяющего центра, изготавливает ключи подписи и сертификат ключа подписи на предоставляемый лицом, проходящим процедуру регистрации, ключевой носитель.

Ответственный сотрудник Оператора Удостоверяющего центра изготавливает две копии сертификата ключа подписи на бумажном носителе по форме, определенной Приложением 11 к настоящему Регламенту. Все копии сертификата открытого ключа на бумажном носителе заверяются собственноручной подписью лица, проходящего процедуру регистрации, или собственноручной подписью доверенного лица, а также собственноручной подписью ответственного сотрудника Оператора Удостоверяющего центра и печатью Оператора Удостоверяющего центра.

По окончании процедуры регистрации Пользователю Удостоверяющего центра выдаются:

ключевой носитель, содержащий:

закрытый и открытый ключ подписи, записанные в виде ключевого контейнера в формате, определяемом средством электронной цифровой подписи.

Дополнительно Пользователю Удостоверяющего центра предоставляются (на дискете 3,5"):

сертификат ключа подписи Пользователя Удостоверяющего центра в электронной форме в виде файла, соответствующий закрытому ключу;

копия сертификата ключа подписи уполномоченного лица Удостоверяющего центра в электронной форме в виде файла;

копия сертификата ключа подписи Пользователя Удостоверяющего центра на бумажном носителе.

9.1.2. Регистрация Пользователя и изготовление первого сертификата в распределенном режиме.

Регистрация Пользователя в распределенном режиме осуществляется на основании заявления на регистрацию по форме Приложения 3 настоящего Регламента. Заявление на регистрацию предоставляется Оператору Удостоверяющего центра посредством почтовой либо курьерской связи (без личного прибытия регистрирующегося лица). Дополнительно регистрирующееся лицо должно предоставить Сведения об ответственных сотрудниках и адресе электронной почты по форме Приложения 4.

После принятия положительного решения о регистрации Оператор Удостоверяющего центра имеет право по заявлению пользователя предоставлять сертификат уполномоченного лица Удостоверяющего центра и актуальный список отозванных сертификатов в виде файлов на магнитном носителе (дискета 3,5"), а также адрес web-страницы регистрации в Удостоверяющем центре.

Пользователь производит установку и настройку своего рабочего места и с помощью автоматизированного рабочего места (АРМ) Пользователя Удостоверяющего центра формирует и направляет запрос на регистрацию в электронной форме в Удостоверяющий центр.

Ответственное лицо Оператора Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на регистрацию, с информацией, содержащейся в запросе на регистрацию, поданном в электронной форме. В случае идентичности указанной идентификационной информации пользователь регистрируется Оператором в Удостоверяющем центре.

Регистрация Пользователя и уведомление Пользователя о регистрации должны быть осуществлены не позднее 3 рабочих дней, следующих за рабочим днем, в течение которого был подан запрос на регистрацию в Удостоверяющий центр в электронном виде.

После получения уведомления о регистрации в Удостоверяющем центре Пользователь с помощью АРМ Пользователя Удостоверяющего центра генерирует пару ключей, формирует и направляет запрос на сертификат открытого ключа в электронной форме в Удостоверяющий центр и подает заявление на изготовление сертификата по форме Приложения 6 к настоящему Регламенту (подача заявления осуществляется посредством почтовой либо курьерской связи).

Допускается прием и обработка заявления, переданного по факсу или по электронной почте, при условии одновременной отправки оригинала заявления через почтовую или курьерскую связь.

Ответственное лицо Оператора Удостоверяющего центра производит сравнение идентификационной информации, указанной в заявлении на изготовление сертификата, с информацией, указанной в запросе на сертификат, поданном в электронной форме. В случае идентичности идентификационной информации ответственное лицо издает сертификат открытого ключа пользователя.

Изготовление сертификата и уведомление Пользователя об изготовлении сертификата должны быть осуществлены не позднее 3 рабочих дней, следующих за рабочим днем, в течение которого был подан запрос на изготовление сертификата в электронном виде.

После получения уведомления об изготовлении сертификата Пользователь с помощью АРМ Пользователя Удостоверяющего центра производит установку сертификата на своем рабочем месте и подтверждает ее.

9.2. Изготовление и получение ключей подписи и сертификата ключа подписи.

Изготовление ключей подписи и сертификата открытого ключа Пользователя Удостоверяющего центра осуществляется при плановой и внеплановой смене закрытого ключа подписи Пользователя Удостоверяющего центра.

Формирование ключей подписи и сертификата ключа подписи Пользователя Удостоверяющего центра осуществляется Оператором Удостоверяющего центра на основании заявления на изготовление сертификата ключа подписи.

Заявление на изготовление сертификата ключа подписи может подаваться в Удостоверяющий центр в бумажной форме при личном прибытии Пользователя Удостоверяющего центра в офис Оператора Удостоверяющего центра либо посредством почтовой или курьерской связи.

Форма заявления на изготовление ключей подписи и сертификата ключа подписи приведена в Приложении 6 к настоящему Регламенту.

В том случае, если Пользователь Удостоверяющего центра не может прибыть лично в офис Оператора Удостоверяющего центра, Сторона, присоединившаяся к Регламенту, должна выдать лицу, пребывающему в офис Оператора Удостоверяющего центра, Доверенность на получение ключей и сертификата ключа подписи соответствующего Пользователя Удостоверяющего центра. Форма Доверенности приведена в Приложении 7 к настоящему Регламенту.

Сторона, присоединившаяся к Регламенту, может направить заявление на изготовление ключей подписи и сертификата ключа подписи в том числе посредством почтовой или курьерской связи. В этом случае заявление направляется в электронной форме с использованием программного обеспечения, предоставляемого Удостоверяющим центром, с одновременным направлением в адрес Оператора заверенной бумажной копии заявления.

При личной явке Пользователя Удостоверяющего центра ответственный сотрудник Оператора Удостоверяющего центра выполняет процедуру идентификации Пользователя Удостоверяющего центра или доверенного лица путем установления личности по паспорту.

После положительной идентификации Пользователя Удостоверяющего центра или доверенного лица ответственный сотрудник Оператора Удостоверяющего центра принимает документы и осуществляет их рассмотрение.

Заявление на изготовление ключей подписи и сертификата открытого ключа рассматривается ответственным сотрудником Оператора Удостоверяющего центра в течение 1 (одного) часа с момента поступления.

В случае отказа в изготовлении ключей подписи и сертификата открытого ключа заявление на изготовление ключей подписи и сертификата открытого ключа вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника Оператора Удостоверяющего центра.

При принятии положительного решения ответственный сотрудник Оператора Удостоверяющего центра изготавливает ключи подписи и сертификат ключа подписи на предоставляемый Пользователем Удостоверяющего центра или его представителем ключевой носитель.

По окончании процедуры изготовления ключей и сертификата ключа подписи Пользователю Удостоверяющего центра выдаются:

ключевой носитель, содержащий:

закрытый и открытый ключ подписи, записанные в виде ключевого контейнера в формате, определяемом средством электронной цифровой подписи;

дополнительно Пользователю Удостоверяющего центра предоставляется (на дискете 3,5") сертификат ключа подписи Пользователя Удостоверяющего центра в электронной форме в виде файла, соответствующий закрытому ключу.

9.3. Аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра.

Для осуществления аннулирования (отзыва) сертификата ключа подписи Пользователь Удостоверяющего центра подает заявление на аннулирование (отзыв) сертификата ключа подписи Оператору Удостоверяющего центра.

Заявление на аннулирование (отзыв) сертификата ключа подписи может подаваться в бумажной форме (при личном прибытии Пользователя Удостоверяющего центра в офис Оператора Удостоверяющего центра либо посредством почтовой или курьерской связи).

Форма заявления на аннулирование (отзыв) сертификата ключа подписи приведена в Приложении 8 к настоящему Регламенту.

Заявление на аннулирование (отзыв) сертификата ключа подписи заверяется собственноручной подписью владельца сертификата ключа подписи (Пользователя Удостоверяющего центра) и подается в офис Оператора Удостоверяющего центра.

Подача заявления и его рассмотрение осуществляются только в течение рабочего дня.

Обработка заявления на аннулирование (отзыв) сертификата ключа подписи и официальное уведомление Пользователя Удостоверяющего центра об аннулировании (отзыве) сертификата ключа подписи должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление Оператору Удостоверяющего центра.

Официальным уведомлением о факте аннулирования (отзыва) сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате. Временем аннулирования (отзыва) сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения об аннулированном (отозванном) сертификате, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

9.4. Приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра.

Для осуществления приостановления действия сертификата ключа подписи Пользователь Удостоверяющего центра подает заявление на приостановление действия сертификата ключа подписи.

Заявление в устной форме делается в офис Оператора Удостоверяющего центра по телефону.

Заявитель должен сообщить ответственному сотруднику Оператора Удостоверяющего центра следующую информацию:

идентификационные данные владельца сертификата ключа подписи;

серийный номер сертификата ключа подписи, действие которого требуется приостановить;

срок, на который приостанавливается действие сертификата ключа подписи;

ключевая фраза Пользователя Удостоверяющего центра (определяемая в процессе регистрации Пользователя Удостоверяющего центра).

Заявление принимается только в случае положительной аутентификации Пользователя Удостоверяющего центра (совпадения ключевой фразы, переданной в заявлении, с информацией из реестра пользователей Удостоверяющего центра).

Заявление в бумажной форме подается в офис Оператора Удостоверяющего центра по форме, приведенной в Приложении 9.

Заявление в бумажной форме содержит следующую информацию:

идентификационные данные владельца сертификата ключа подписи;

серийный номер сертификата ключа подписи, действие которого требуется приостановить;

срок, на который приостанавливается действие сертификата ключа подписи;

дата и время подачи заявления.

Заявление на приостановление действия сертификата ключа подписи заверяется собственноручной подписью владельца сертификата (Пользователя Удостоверяющего центра) и подается в офис Оператора Удостоверяющего центра (при личном прибытии заявителя либо посредством почтовой или курьерской связи).

Действие сертификата приостанавливается на исчисляемый в днях срок. Минимальный срок приостановления действия сертификата составляет 10 (десять) дней.

Подача заявления на приостановление действия сертификата в Удостоверяющий центр и его рассмотрение осуществляются только в течение рабочего дня.

Обработка заявления на приостановление действия сертификата ключа подписи и оповещение Пользователя Удостоверяющего центра о приостановлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Официальным уведомлением о приостановлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено. Временем приостановления действия сертификата ключа подписи признается время издания списка отозванных сертификатов, содержащего сведения о сертификате, действие которого было приостановлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

В том случае, если в течение срока приостановления действия сертификата ключа подписи Пользователя Удостоверяющего центра Оператору Удостоверяющего центра не поступает заявление от Пользователя Удостоверяющего центра о возобновлении действия сертификата, сертификат аннулируется (отзывается) Удостоверяющим центром.

9.5. Возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра.

Для осуществления возобновления действия сертификата ключа подписи Пользователь Удостоверяющего центра подает заявление на возобновление действия сертификата.

Возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра осуществляется ответственным сотрудником Оператора Удостоверяющего центра на основании заявления на возобновление действия сертификата ключа подписи, поступающего в бумажной форме.

Заявление в бумажной форме подается в офис Оператора Удостоверяющего центра по форме, приведенной в Приложении 10.

Заявление в бумажной форме содержит следующую информацию:

идентификационные данные владельца сертификата ключа подписи;

серийный номер сертификата ключа подписи, действие которого требуется возобновить;

дату и время подачи заявления.

Заявление на возобновление действия сертификата ключа подписи в бумажной форме заверяется собственноручной подписью владельца сертификата (Пользователя Удостоверяющего центра) и подается в офис Оператора Удостоверяющего центра (при личном прибытии заявителя либо посредством почтовой или курьерской связи).

Подача заявления на возобновление действия сертификата в Удостоверяющий центр и его рассмотрение осуществляются только в течение рабочего дня.

Обработка заявления на возобновление действия сертификата и оповещение Пользователя Удостоверяющего центра о возобновлении действия сертификата должны быть осуществлены не позднее одного рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий центр.

Официальным уведомлением о возобновлении действия сертификата ключа подписи является опубликование списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено. Временем возобновления действия сертификата ключа подписи признается время издания списка отозванных сертификатов, не содержащего сведений о сертификате, действие которого было возобновлено, указанное в поле thisUpdate изданного списка отозванных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим центром сертификаты ключа подписи в поле CRL Distribution Point.

9.6. Подтверждение подлинности ЭЦП в электронном документе. Для подтверждения подлинности ЭЦП в электронных документах, циркулирующих в Информационной системе, Пользователь Удостоверяющего центра подает Заявление на подтверждение подлинности ЭЦП в электронном документе в офис Оператора Удостоверяющего центра.

Подтверждение подлинности ЭЦП электронного документа осуществляется на основании заявления, содержащего следующую информацию:

дата и время подачи заявления;

идентификационные данные Пользователя Удостоверяющего центра, ЭЦП которого требуется проверить в электронном документе;

серийный номер сертификата ключа подписи, на котором требуется проверить ЭЦП электронного документа;

дата и время формирования ЭЦП в электронном документе. Обязательным приложением к заявлению на подтверждение подлинности ЭЦП в электронном документе является файл на сменном магнитном носителе, содержащий электронный документ.

Предоставляемый файл получается путем экспорта электронного документа, к которому применена ЭЦП, из Информационной системы.

Электронная цифровая подпись в предоставленном электронном документе будет считаться равнозначной собственноручной подписи при выполнении следующих условий:

сертификат ключа подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭЦП, не утратил силу (действует) на момент формирования ЭЦП в электронном документе - дата и время формирования ЭЦП в электронном документе, указанные в заявлении на подтверждение подлинности ЭЦП;

ЭЦП, проверенная на сертификате ключа подписи с серийным номером, указанным в заявлении на подтверждение подлинности ЭЦП, верна;

ЭЦП используется в соответствии со сведениями, указанными в сертификате ключа подписи - в поле Extended Key Usage;

формирование ЭЦП осуществлено без нарушений условий настоящего Регламента.

Срок проведения работ по заявлению на подтверждение подлинности ЭЦП в электронном документе и предоставлению заключения о произведенной проверке составляет 15 (пятнадцать) рабочих дней с момента его предоставления Оператору Удостоверяющего центра.

Проведение работ по подтверждению подлинности ЭЦП в электронном документе осуществляет комиссия, сформированная из числа сотрудников Оператора Удостоверяющего центра. При проведении указанных работ Оператор Удостоверяющего центра (комиссия) имеет право привлекать к проведению экспертных работ специалистов Удостоверяющего центра.

Результатом проведения работ по подтверждению подлинности ЭЦП в электронном документе является заключение в письменной форме, подписанное всеми членами комиссии и заверенное печатью Оператора Удостоверяющего центра.

Заключение содержит:

результат проверки ЭЦП электронного документа;

отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

время и место проведения проверки;

состав комиссии, осуществлявшей проверку;

основание для проведения проверки;

содержание и результаты проверки с указанием примененных методов;

обоснование результатов проверки;

данные, представленные комиссии для проведения проверки.

Отчет по выполненной проверке составляется в простой письменной форме и заверяется собственноручными подписями всех членов комиссии.

9.7. Подтверждение подлинности ЭЦП уполномоченного лица Удостоверяющего центра в изданных сертификатах.

Для подтверждения подлинности ЭЦП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи Пользователь Удостоверяющего центра подает заявление на подтверждение подлинности ЭЦП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи Оператору Удостоверяющего центра.

Заявление должно содержать следующую информацию:

дата и время подачи заявления;

идентификационные данные субъекта, в сертификате ключа подписи которого необходимо подтвердить ЭЦП уполномоченного лица Удостоверяющего центра;

серийный номер сертификата ключа подписи, в котором необходимо подтвердить ЭЦП уполномоченного лица Удостоверяющего центра.

Обязательным приложением к заявлению на подтверждение подлинности ЭЦП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи является сменный магнитный носитель, содержащий файл сертификата ключа подписи, подвергающегося процедуре проверки.

Срок проведения работ по подтверждению подлинности ЭЦП и предоставлению заключения о произведенной проверке составляет 15 (пятнадцать) рабочих дней с момента его предоставления Оператору Удостоверяющего центра.

На основании полученного заявления Оператор Удостоверяющего центра установленным порядком обращается в Удостоверяющий центр, который осуществляет подтверждение подлинности ЭЦП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи.

Результатом проведения работ по подтверждению подлинности ЭЦП уполномоченного лица Удостоверяющего центра в сертификате ключа подписи является заключение Удостоверяющего центра в письменной форме, подписанное уполномоченным лицом Удостоверяющего центра и заверенное печатью Удостоверяющего центра.

Заключение содержит:

результат проверки ЭЦП уполномоченного лица Удостоверяющего центра;

отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

время и место проведения проверки;

основание для проведения проверки;

содержание и результаты проверки с указанием примененных методов;

обоснование результатов проверки;

данные, представленные для проведения проверки.

Отчет по выполненной проверке составляется в простой письменной форме.

9.8. Прочие условия.

9.8.1. Регистрация Пользователя может быть осуществлена уполномоченным представителем Пользователя Удостоверяющего центра, действующим на основании доверенности на осуществление регистрации в Удостоверяющем центре. Доверенность на осуществление регистрации в Удостоверяющем центре должна быть составлена и оформлена по форме Приложения 5 настоящего Регламента.

9.8.2. Период времени действия закрытого ключа, соответствующего выданному сертификату ключа подписи Пользователя Удостоверяющего центра, должен находиться в пределах периода времени, на который выдана Стороной, присоединившейся к Регламенту, соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента для Пользователя Удостоверяющего центра.

### 10. Структура сертификатов ключей подписи и сроки действия ключевых документов

10.1. Структура сертификата ключа подписи уполномоченного лица Удостоверяющего центра.

---------------------------------------------------------------------------

¦ Название ¦ Описание ¦ Содержание ¦

+---------------+-----------------+---------------------------------------+

¦ Базовые поля сертификата ¦

+-------------------------------------------------------------------------+

¦Version ¦Версия ¦V3 ¦

+---------------+-----------------+---------------------------------------+

¦Serial Number ¦Серийный номер ¦Уникальный серийный номер сертификата ¦

+---------------+-----------------+---------------------------------------+

¦Signature ¦Алгоритм подписи ¦ГОСТ Р 34.11/34.10-2001 ¦

¦Algorithm ¦ ¦ ¦

+---------------+-----------------+---------------------------------------+

¦Issuer ¦Издатель ¦CommonName - УЦ КРИПТО-ПРО - ¦

¦ ¦сертификата ¦псевдоним уполномоченного лица ¦

¦ ¦ ¦Удостоверяющего центра ¦

¦ ¦ ¦Organization (организация) - ¦

¦ ¦ ¦ООО КРИПТО-ПРО ¦

¦ ¦ ¦Locality (город) - Москва ¦

¦ ¦ ¦Country (страна) - RU ¦

¦ ¦ ¦Email (электронная почта) - ¦

¦ ¦ ¦cpca@cryptopro.ru ¦

+---------------+-----------------+---------------------------------------+

¦Validity ¦Срок действия ¦Действителен с (notBefore): дд.мм.гггг ¦

¦Period ¦сертификата ¦чч:мм:сс GMT ¦

¦ ¦ ¦ Действителен по (notAfter): дд.мм.гггг¦

¦ ¦ ¦чч:мм:сс GMT ¦

+---------------+-----------------+---------------------------------------+

¦Subject ¦Владелец ¦CommonName - УЦ КРИПТО-ПРО - ¦

¦ ¦сертификата ¦псевдоним уполномоченного лица ¦

¦ ¦ ¦Удостоверяющего центра ¦

¦ ¦ ¦Organization (организация) - ¦

¦ ¦ ¦ООО КРИПТО-ПРО ¦

¦ ¦ ¦Locality (город) - Москва ¦

¦ ¦ ¦Country (страна) - RU ¦

¦ ¦ ¦Email (электронная почта) - ¦

¦ ¦ ¦cpca@cryptopro.ru ¦

+---------------+-----------------+---------------------------------------+

¦Public Key ¦Открытый ключ ¦Открытый ключ (алгоритм ¦

¦ ¦ ¦ГОСТ Р 34.10-2001) ¦

+---------------+-----------------+---------------------------------------+

¦Issuer ¦Алгоритм подписи ¦ГОСТ Р 34.11/34.10-2001 ¦

¦Signature ¦издателя ¦ ¦

¦Algorithm ¦сертификата ¦ ¦

+---------------+-----------------+---------------------------------------+

¦Issuer Sign ¦ЭЦП издателя ¦Подпись издателя в соответствии с ¦

¦ ¦сертификата ¦ГОСТ Р 34.11/34.10-2001 ¦

+---------------+-----------------+---------------------------------------+

¦ ¦ Дополнения сертификата ¦

+---------------+---------------------------------------------------------+

¦Key Usage ¦Использование ¦Неотрекаемость - невозможность ¦

¦(critical) ¦ключа ¦осуществления отказа от совершенных ¦

¦ ¦ ¦действий. ¦

¦ ¦ ¦Подписание сертификатов, автономное ¦

¦ ¦ ¦подписание списка отзыва (CRL), ¦

¦ ¦ ¦подписание списка отзыва (CRL) ¦

+---------------+-----------------+---------------------------------------+

¦Subject Key ¦Идентификатор ¦Идентификатор закрытого ключа ¦

¦Idendifier ¦ключа владельца ¦уполномоченного лица Удостоверяющего ¦

¦ ¦сертификата ¦центра, соответствующего данному ¦

¦ ¦ ¦сертификату ¦

+---------------+-----------------+---------------------------------------+

¦BasicCon- ¦Основные ¦SybjectType (тип владельца ¦

¦straints ¦ограничения ¦сертификата) - ЦС ¦

¦ ¦ ¦Path Length Constraint (ограничение на ¦

¦ ¦ ¦длину пути - ограничивает количество ¦

¦ ¦ ¦уровней иерархии при создании ¦

¦ ¦ ¦подчиненных Удостоверяющих центров) - ¦

¦ ¦ ¦отсутствует ¦

+---------------+-----------------+---------------------------------------+

¦SzOID\_ ¦Объектный ¦Версия сертификата уполномоченного ¦

¦CertSrv\_ ¦идентификатор ¦лица Удостоверяющего центра ¦

¦CA\_Version ¦версии ¦ ¦

¦ ¦сертификата ¦ ¦

----------------+-----------------+----------------------------------------

10.2. Структура сертификата ключа подписи Пользователя Удостоверяющего центра.

---------------------------------------------------------------------------

¦ Название ¦ Описание ¦ Содержание ¦

+-----------------+------------------+------------------------------------+

¦ Базовые поля сертификата ¦

+-------------------------------------------------------------------------+

¦Version ¦Версия ¦V3 ¦

+-----------------+------------------+------------------------------------+

¦Serial ¦Серийный номер ¦Уникальный серийный номер ¦

¦Number ¦ ¦сертификата ¦

+-----------------+------------------+------------------------------------+

¦Signature ¦Алгоритм подписи ¦ГОСТ Р 34.11/34.10-2001 ¦

¦Algorithm ¦ ¦ ¦

+-----------------+------------------+------------------------------------+

¦Issuer ¦Издатель ¦CommonName - УЦ КРИПТО-ПРО - ¦

¦ ¦сертификата ¦псевдоним уполномоченного лица ¦

¦ ¦ ¦Удостоверяющего центра ¦

¦ ¦ ¦Organization (организация) - ООО ¦

¦ ¦ ¦КРИПТО-ПРО ¦

¦ ¦ ¦Locality (город) - Москва ¦

¦ ¦ ¦Country (страна) - RU ¦

¦ ¦ ¦Email (электронная почта) - ¦

¦ ¦ ¦cpca@cryptopro.ru ¦

+-----------------+------------------+------------------------------------+

¦Validity ¦Срок действия ¦Действителен с (notBefore): ¦

¦Period ¦сертификата ¦дд.мм.гггг чч:мм:сс GMT ¦

¦ ¦ ¦Действителен по (notAfter): ¦

¦ ¦ ¦дд.мм.гггг чч:мм:сс GMT ¦

+-----------------+------------------+------------------------------------+

¦Subject ¦Владелец ¦CommonName - фамилия, имя, отчество ¦

¦ ¦сертификата ¦или псевдоним ¦

¦ ¦ ¦OrganizationUnit - подразделение ¦

¦ ¦ ¦Organization - организация ¦

¦ ¦ ¦Title - должность ¦

¦ ¦ ¦Locality - город ¦

¦ ¦ ¦State - субъект РФ ¦

¦ ¦ ¦Country - страна - RU ¦

¦ ¦ ¦Email - электронная почта ¦

¦ ¦ ¦Компонента имени CN обязательна для ¦

¦ ¦ ¦заполнения, необходимость заполнения¦

¦ ¦ ¦остальных значений определяется ¦

¦ ¦ ¦владельцем сертификата и Оператором ¦

¦ ¦ ¦Удостоверяющего центра. В поле ¦

¦ ¦ ¦Subject сертификата могут быть ¦

¦ ¦ ¦добавлены дополнительные компоненты ¦

¦ ¦ ¦имени согласно RFC 3280 ¦

+-----------------+------------------+------------------------------------+

¦Public Key ¦Открытый ключ ¦Открытый ключ (алгоритм подписи) ¦

+-----------------+------------------+------------------------------------+

¦Issuer ¦Алгоритм подписи ¦ГОСТ Р 34.11/34.10-2001 ¦

¦Signature ¦издателя ¦ ¦

¦Algorithm ¦сертификата ¦ ¦

+-----------------+------------------+------------------------------------+

¦Issuer Sign ¦ЭЦП издателя ¦Подпись издателя в соответствии с ¦

¦ ¦сертификата ¦ГОСТ Р 34.11/34.10-2001 ¦

+-----------------+------------------+------------------------------------+

¦ Расширения сертификата ¦

+-------------------------------------------------------------------------+

¦Key Usage ¦Использование ¦Неотрекаемость - невозможность ¦

¦(critical) ¦ключа ¦осуществления отказа от совершенных ¦

¦ ¦ ¦действий. ¦

¦ ¦ ¦Цифровая подпись, шифрование ¦

¦ ¦ ¦ключей, шифрование данных ¦

+-----------------+------------------+------------------------------------+

¦Extended Key ¦Улучшенный ключ ¦Набор областей использования ключей ¦

¦Usage ¦ ¦и сертификатов из перечня областей ¦

¦ ¦ ¦использования, зарегистрированных в ¦

¦ ¦ ¦Удостоверяющем центре ¦

+-----------------+------------------+------------------------------------+

¦Application ¦Политика ¦Набор областей использования ключей ¦

¦Policy ¦применения ¦и сертификатов из перечня областей ¦

¦ ¦ ¦использования, зарегистрированных в ¦

¦ ¦ ¦Удостоверяющем центре ¦

+-----------------+------------------+------------------------------------+

¦Subject ¦Идентификатор ¦Идентификатор закрытого ключа ¦

¦Key ¦ключа владельца ¦владельца сертификата ¦

¦Idendifier ¦сертификата ¦ ¦

+-----------------+------------------+------------------------------------+

¦Authority ¦Идентификатор ¦Идентификатор закрытого ключа ¦

¦Key ¦ключа издателя ¦Уполномоченного лица ¦

¦Identifier ¦сертификата ¦Удостоверяющего центра, на котором ¦

¦ ¦ ¦подписан данный сертификат ¦

+-----------------+------------------+------------------------------------+

¦CRL Distribution ¦Точка ¦Набор адресов точек распространения ¦

¦Point ¦распространения ¦списков отозванных сертификатов ¦

¦ ¦списка отозванных ¦следующего вида: ¦

¦ ¦сертификатов ¦URL: http://ResourceServer/ ¦

¦ ¦ ¦Path/hex.crl, где ResourceServer - ¦

¦ ¦ ¦имя сервера, Path - путь к файлу ¦

¦ ¦ ¦списка отозванных сертификатов, hex ¦

¦ ¦ ¦- шестнадцатеричное значение ¦

¦ ¦ ¦идентификатора закрытого ключа ¦

¦ ¦ ¦уполномоченного лица ¦

¦ ¦ ¦Удостоверяющего центра, с ¦

¦ ¦ ¦использованием которого издан ¦

¦ ¦ ¦сертификат и список отозванных ¦

¦ ¦ ¦сертификатов ¦

+-----------------+------------------+------------------------------------+

¦Authority ¦Адрес Службы ¦URL адреса web-приложения Службы ¦

¦Information ¦актуальных ¦актуальных статусов сертификатов. ¦

¦Access ¦статусов ¦Заносится в сертификаты, статус ¦

¦ ¦сертификатов ¦которых может быть установлен по ¦

¦ ¦ ¦протоколу OCSP ¦

+-----------------+------------------+------------------------------------+

¦ ¦ ¦В сертификат ключа подписи могут ¦

¦ ¦ ¦быть добавлены дополнительные поля ¦

¦ ¦ ¦и расширения согласно RFC 3280 ¦

------------------+------------------+-------------------------------------

10.3. Структура списка отозванных сертификатов (CRL) Удостоверяющего центра.

---------------------------------------------------------------------------

¦ Название ¦ Описание ¦ Содержание ¦

+---------------+-------------------+-------------------------------------+

¦ Базовые поля списка отозванных сертификатов ¦

+-------------------------------------------------------------------------+

¦Version ¦Версия ¦V2 ¦

+---------------+-------------------+-------------------------------------+

¦Issuer ¦Издатель СОС ¦CommonName - УЦ КРИПТО-ПРО - ¦

¦ ¦ ¦псевдоним уполномоченного лица ¦

¦ ¦ ¦Удостоверяющего центра ¦

¦ ¦ ¦Organization (организация) - ¦

¦ ¦ ¦ООО КРИПТО-ПРО ¦

¦ ¦ ¦Locality (город) - Москва ¦

¦ ¦ ¦Country (страна) - RU ¦

¦ ¦ ¦Email (электронная почта) - ¦

¦ ¦ ¦cpca@cryptopro.ru ¦

+---------------+-------------------+-------------------------------------+

¦thisUpdate ¦Время издания СОС ¦дд.мм.гггг чч:мм:сс GMT ¦

+---------------+-------------------+-------------------------------------+

¦nextUpdate ¦Время, по которое ¦дд.мм.гггг чч:мм:сс GMT ¦

¦ ¦действителен СОС ¦ ¦

+---------------+-------------------+-------------------------------------+

¦revoked ¦Список отозванных ¦Последовательность элементов ¦

¦Certificates ¦сертификатов ¦следующего вида: ¦

¦ ¦ ¦1) серийный номер сертификата ¦

¦ ¦ ¦(CertificateSerialNumber); ¦

¦ ¦ ¦2) время обработки заявления на ¦

¦ ¦ ¦аннулирование (отзыв) сертификата ¦

¦ ¦ ¦(Time); ¦

¦ ¦ ¦3) код причины отзыва сертификата ¦

¦ ¦ ¦(Reson Code): ¦

¦ ¦ ¦"0" не указана ¦

¦ ¦ ¦"1" компрометация ключа ¦

¦ ¦ ¦"2" компрометация ЦС ¦

¦ ¦ ¦"3" изменение принадлежности ¦

¦ ¦ ¦"4" сертификат заменен ¦

¦ ¦ ¦"5" прекращение работы ¦

¦ ¦ ¦"6" приостановка действия ¦

+---------------+-------------------+-------------------------------------+

¦signature ¦Алгоритм подписи ¦ГОСТ Р 34.11/34.10-2001 ¦

¦Algorithm ¦ ¦ ¦

+---------------+-------------------+-------------------------------------+

¦Issuer Sign ¦Подпись издателя ¦Подпись издателя в соответствии с ¦

¦ ¦СОС ¦ГОСТ Р 34.11/34.10-2001 ¦

+---------------+-------------------+-------------------------------------+

¦ Расширения списка отозванных сертификатов ¦

+-------------------------------------------------------------------------+

¦Authority ¦Идентификатор ¦Идентификатор закрытого ключа ¦

¦Key ¦ключа издателя ¦уполномоченного лица Удостоверяющего ¦

¦Identifier ¦ ¦центра, на котором подписан СОС ¦

+---------------+-------------------+-------------------------------------+

¦SzOID\_ ¦Объектный ¦Версия сертификата уполномоченного ¦

¦CertSrv\_ ¦идентификатор ¦лица Удостоверяющего центра ¦

¦CA\_Version ¦сертификата ¦ ¦

¦ ¦издателя ¦ ¦

----------------+-------------------+--------------------------------------

10.4. Расширения Key Usage, Extended Key Usage, Application Policy сертификата ключа подписи содержат сведения об отношениях, при которых электронный документ будет иметь юридическое значение. Наличие в сертификате ключа подписи области использования "Пользователь Центра Регистрации (1.2.643.2.2.34.6)" устанавливает, что владелец указанного сертификата имеет право подписывать ЭЦП электронные документы, определенные настоящим Регламентом для Пользователя Удостоверяющего центра.

10.5. Сроки действия ключевых документов.

10.5.1. Срок действия закрытого ключа уполномоченного лица Удостоверяющего центра составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности Удостоверяющего центра и для средства ЭЦП, с использованием которого данный закрытый ключ был сформирован.

Начало периода действия закрытого ключа уполномоченного лица Удостоверяющего центра исчисляется с даты и времени генерации закрытого ключа уполномоченного лица Удостоверяющего центра.

Срок действия сертификата ключа подписи Уполномоченного лица Удостоверяющего центра не превышает 30 (тридцати) лет. Время начала периода действия сертификата ключа подписи уполномоченного лица Удостоверяющего центра и его окончания заносится в поля "notBefore" и "notAfter" поля "Validity Period" соответственно.

Срок действия закрытого ключа Пользователя Удостоверяющего Центра составляет 1 (один) год.

10.5.2. Начало периода действия закрытого ключа Пользователя Удостоверяющего центра исчисляется с даты и времени начала действия соответствующего сертификата ключа подписи.

Срок действия сертификата ключа подписи Пользователя Удостоверяющего центра не превышает 30 (тридцати) лет. Время начала периода действия сертификата ключа подписи Пользователя Удостоверяющего центра и его окончания заносится в поля "notBefore" и "notAfter" поля "Validity Period" соответственно.

### 11. Дополнительные положения

11.1. Плановая смена ключей уполномоченного лица Удостоверяющего центра.

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица Удостоверяющего центра выполняется в период действия закрытого ключа уполномоченного лица Удостоверяющего центра.

Процедура плановой смены ключей уполномоченного лица Удостоверяющего центра осуществляется в следующем порядке:

уполномоченное лицо Удостоверяющего центра генерирует новый закрытый и соответствующий ему открытый ключ;

уполномоченное лицо Удостоверяющего центра изготавливает новый сертификат ключа подписи уполномоченного лица Удостоверяющего центра.

Старый закрытый ключ уполномоченного лица Удостоверяющего центра используется в течение своего срока действия для формирования списков отозванных сертификатов, изданных Удостоверяющим центром в период действия старого закрытого ключа уполномоченного лица Удостоверяющего центра.

По истечении одного года с момента проведения плановой смены ключей уполномоченного лица Удостоверяющий центр изготавливает список отозванных сертификатов, соответствующий старому закрытому ключу, со сроком действия, соответствующим сроку действия старого сертификата уполномоченного лица Удостоверяющего центра (значение поля nextUpdate списка отозванных сертификатов совпадает со значением поля notAfter поля Validity сертификата ключа подписи уполномоченного лица Удостоверяющего центра). Изданный список отозванных сертификатов публикуется Удостоверяющим центром, изготовление нового списка отозванных сертификатов, соответствующего старому закрытому ключу уполномоченного лица Удостоверяющего центра, более не осуществляется.

11.2. Компрометация ключевых документов уполномоченного лица Удостоверяющего центра, внеплановая смена ключей уполномоченного лица Удостоверяющего центра.

В случае компрометации закрытого ключа уполномоченного лица Удостоверяющего центра сертификат уполномоченного лица Удостоверяющего центра аннулируется (отзывается), Пользователи Удостоверяющего центра уведомляются об указанном факте путем рассылки соответствующего уведомления по электронной почте и публикации информации о компрометации на сайте Удостоверяющего центра. Все сертификаты, изданные с использованием скомпрометированного ключа уполномоченного лица Удостоверяющего центра, считаются аннулированными.

После аннулирования сертификата уполномоченного лица Удостоверяющего центра выполняется процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра. Процедура внеплановой смены ключей уполномоченного лица Удостоверяющего центра выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица Удостоверяющего центра.

Все действовавшие на момент компрометации закрытого ключа уполномоченного лица Удостоверяющего центра сертификаты ключей подписей, а также сертификаты, действие которых было приостановлено, подлежат внеплановой смене.

11.3. Компрометация ключевых документов Пользователя Удостоверяющего центра.

Пользователь Удостоверяющего центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа.

В случае компрометации или угрозы компрометации закрытого ключа Пользователь связывается с Оператором по телефону и сообщает ему:

свои идентификационные данные;

серийный номер сертификата ключа подписи, соответствующего скомпрометированному ключу;

секретное ключевое слово, полученное при регистрации.

Оператор производит аутентификацию Пользователя Удостоверяющего центра по секретному ключевому слову.

В случае успешной аутентификации Оператор приостанавливает действие сертификата на 30 (тридцать) календарных дней.

Если в течение срока приостановления действия сертификата ключа подписи Пользователь не направит в Удостоверяющий центр заявление на возобновление действия сертификата, то Удостоверяющий центр автоматически аннулирует (отзовет) данный сертификат.

Пользователь Удостоверяющего центра осуществляет внеплановую смену ключей в соответствии с пунктом 11.2 настоящего Регламента.

11.4. Конфиденциальность информации.

11.4.1. Типы конфиденциальной информации.

11.4.1.1. Закрытый ключ, соответствующий сертификату ключа подписи, является конфиденциальной информацией лица, зарегистрированного в Удостоверяющем центре. Оператор не осуществляет хранение закрытых ключей Пользователей Удостоверяющего центра.

11.4.1.2. Персональная и корпоративная информация о лицах, зарегистрированных в Удостоверяющем центре и содержащаяся в Реестре Удостоверяющего центра, не подлежащая непосредственной рассылке в качестве части сертификата ключа подписи, считается конфиденциальной.

11.4.2. Типы информации, не являющейся конфиденциальной.

11.4.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

11.4.2.2. Открытая информация может публиковаться по решению Оператора и Удостоверяющего центра. Место, способ и время публикации открытой информации определяются Оператором и Удостоверяющим центром.

11.4.2.3. Информация, включаемая в сертификаты ключей подписи и списки отозванных сертификатов, издаваемые Удостоверяющим центром, не считается конфиденциальной.

11.4.2.4. Персональные данные, включаемые в сертификаты ключей подписей, издаваемые Удостоверяющим центром, относятся к общедоступным персональным данным.

11.4.2.5. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

11.4.3. Исключительные полномочия Оператора и Удостоверяющего центра.

11.4.3.1. Оператор и Удостоверяющий центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством Российской Федерации.

11.5. Форс-мажор.

11.5.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Регламенту, если это неисполнение явилось следствием форс-мажорных обстоятельств, возникших после присоединения к настоящему Регламенту.

11.5.2. Форс-мажорными обстоятельствами признаются чрезвычайные (т.е. находящиеся вне разумного контроля Сторон) и непредотвратимые при данных условиях обстоятельства, включая военные действия, массовые беспорядки, стихийные бедствия, забастовки, технические сбои функционирования программного обеспечения, пожары, взрывы и иные техногенные катастрофы, действия (бездействие) государственных и муниципальных органов, повлекшие невозможность исполнения Стороной/Сторонами своих обязательств по настоящему Регламенту.

11.5.3. В случае возникновения форс-мажорных обстоятельств срок исполнения Сторонами своих обязательств по настоящему Регламенту отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

11.5.4. Сторона, для которой создалась невозможность исполнения своих обязательств по настоящему Регламенту, должна немедленно известить в письменной форме другую Сторону о наступлении, предполагаемом сроке действия и прекращении форс-мажорных обстоятельств, а также представить доказательства существования названных обстоятельств.

11.5.5. Неизвещение или несвоевременное извещение о наступлении обстоятельств непреодолимой силы влечет за собой утрату права ссылаться на эти обстоятельства.

11.5.6. В случае если невозможность полного или частичного исполнения Сторонами какого-либо обязательства по настоящему Регламенту обусловлена действием форс-мажорных обстоятельств и существует свыше одного месяца, то каждая из Сторон вправе отказаться в одностороннем порядке от дальнейшего исполнения этого обязательства, и в этом случае ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

### 12. Список приложений

12.1. Приложение 1. Подписной лист к Регламенту предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО".

12.2. Приложение 2. Список объектных идентификаторов (OID), зарегистрированных в Удостоверяющем центре ООО "КРИПТО-ПРО", определяющих отношения, при осуществлении которых электронный документ с электронной цифровой подписью будет иметь юридическое значение.

12.3. Приложение 3. Заявление на регистрацию Пользователя в Удостоверяющем центре ООО "КРИПТО-ПРО".

12.4. Приложение 4. Форма доверенности Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО" на осуществление действий в рамках Регламента предоставления услуг Оператора Удостоверяющего центра ООО "КРИПТО-ПРО".

12.5. Приложение 5. Форма доверенности на осуществление регистрации Пользователя в Удостоверяющем центре ООО "КРИПТО-ПРО".

12.6. Приложение 6. Заявление на изготовление сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО".

12.7. Приложение 7. Форма доверенности на получение ключей подписи и сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО".

12.8. Приложение 8. Заявление на аннулирование (отзыв) сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО".

12.9. Приложение 9. Заявление на приостановление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО".

12.10. Приложение 10. Заявление на возобновление действия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО".

12.11. Приложение 11. Копия сертификата ключа подписи Пользователя Удостоверяющего центра ООО "КРИПТО-ПРО" (пример).

Источник - "Научно-практический комментарий к Федеральному закону "О кредитных историях" (постатейный), "Норма", "Инфра-М"

Сохраните в закладки наш сайт: [Порядокправа.рф](https://порядокправа.рф)

Прямая ссылка на документ: [https://порядокправа.рф/obrazecy/reglament\_predostavleniya\_uslug\_operatora\_udostoveryayushhego\_centra\_ooo\_kripto\_pro\_prilozhenie\_k\_sogla.htm](https://порядокправа.рф/reglament_predostavleniya_uslug_operatora_udostoveryayushhego_centra_ooo_kripto_pro_prilozhenie_k_sogla.htm)