

ООО «ОТКРЫТЫЕ АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ»

ИНН 7203355594 / КПП 720301001

E-Mail: director@oas.su

<https://oas.su>


Тел: +7 932 200 96 52

УТВЕРЖДАЮ:

Директор ООО «ОАС»

Баталин Иван Анатольевич

редакция 1.0 от 1 августа 2017 г.



**РЕГЛАМЕНТ
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
ООО «ОАС»**

Разработан: Баталином И.А., Баталиной О.С.

г. Тюмень, 2017 год

ТЕРМИНОЛОГИЯ

Электронная подпись — 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.

Идентификатор — уникальная последовательность байт, однозначно указывающая на принадлежность электронной подписи.

Усиленная электронная подпись — электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, и которая позволяет определить лицо, подписавшее электронный документ, обнаружить факт внесения изменений в электронный документ после момента его подписания.

Ключ ЭП — уникальная последовательность байт, предназначенная для создания усиленной электронной подписи.

Ключ проверки ЭП — уникальная последовательность байт, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности усиленной электронной подписи.

Владелец Ключа ЭП — Физическое или Юридическое Лицо, выпустившее Ключ ЭП и соответствующий ему Ключ проверки ЭП, и имеющий право на единоличное использование Ключа ЭП.

Компрометация Ключа ЭП — доступ постороннего лица к Ключу ЭП.

Удостоверяющий Центр — подразделение ООО «ОАС», осуществляющее функции по созданию и выпуску Сертификатов ключей проверки электронной подписи, а также иные функции, предусмотренные настоящим Регламентом.

Сертификат ключа проверки электронной подписи (далее Сертификат) — электронный документ, выпущенный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи Субъекту Сертификата ключа проверки электронной подписи.

Реестр аннулированных Сертификатов — электронный документ с электронной подписью Удостоверяющего Центра, включающий в себя список серийных номеров аннулированных Сертификатов ключей проверки электронной подписи, информацию о датах и причинах аннулирования Сертификатов ключей проверки электронных подписей.

Реестр актуальных Сертификатов — база данных, ведущаяся Удостоверяющим Центром, включающая в себя список серийных номеров действующих Сертификатов ключей проверки электронных подписей, обезличенную информацию о Субъектах Сертификатов ключей проверки электронных подписей.

Автоматизированная система Удостоверяющего Центра — комплекс программных и аппаратных средств Удостоверяющего Центра, предназначенный для осуществления функций автоматического контроля выпуска, аннулирования и ведения Реестров актуальных и аннулированных Сертификатов ключей электронной подписи, а также предоставления доступа к этим Реестрам согласно настоящему Регламенту.

Контейнер — электронное (в форматах PKCS12 или PKCS15) хранилище или часть физического (смарт-карта либо криптографический токен) хранилища Сертификата ключа проверки электронной подписи и Ключа электронной подписи, защищенное паролем, одноразовым паролем, пин-кодом или электронной подписью.

Головной УЦ — удостоверяющий центр, являющийся доверенным для всех участников Системы Электронного Взаимодействия и не требующий удостоверения другим Удостоверяющим центром.

Подчиненный УЦ — удостоверяющий центр, Сертификат которого выпущен вышестоящим Удостоверяющим Центром для целей выпуска Сертификатов определенного назначения.

Субъект — совокупность полей Сертификата, указывающая на Физическое Лицо, Юридическое Лицо, Оборудование или Программное Обеспечение, в отношении которого выпущен Сертификат.

Аутентификация — процесс проверки подлинности уникального идентификатора Субъекта и подтверждения его владения Субъектом.

Авторизация — процесс предоставления привилегий доступа в Системе Электронного Взаимодействия.

Аннулирование — процесс внесения серийного номера Сертификата ключа электронной подписи в Реестр аннулированных Сертификатов.

Валидация — процесс проверки сроков действия Сертификата, подлинности Подписи Удостоверяющего Центра, выпустившего Сертификат, и отсутствия серийного номера Сертификата в Реестре аннулированных Сертификатов на дату проверки Сертификата или дату Подписания электронного документа этим Сертификатом.

Шифрование — процесс обратимого изменения информации, исключая случайный или преднамеренный доступ к передаваемой информации без специальных технических средств.

Подписание — процесс установки дополнительной информации на основе Сертификата ключа проверки электронной подписи и Ключа электронной подписи.

Отпечаток Сертификата — Уникальная последовательность байт, являющаяся результатом работы криптографической хеширующей функции над файлом Сертификата, сохраненном в формате DER, являющаяся однозначным Идентификатором Сертификата и обеспечивающей уникальность результата работы такой криптографической хеширующей функции.

Средства криптографической защиты информации — программное обеспечение, используемое для целей создания Ключа электронной подписи, Ключа проверки электронной подписи, выпуска Сертификата ключа проверки электронной подписи, а также Валидации, Подписания и Шифрования.

Средства Удостоверяющего Центра — средства криптографической защиты информации, применяемые Удостоверяющим Центром и Автоматизированной системой Удостоверяющего Центра для осуществления функций Удостоверяющего Центра.

Средства Электронной Подписи — средства криптографической защиты информации, применяемые Владельцами Ключей Электронной Подписи и Субъектами для целей создания Ключа Электронной Подписи, соответствующего ему Ключа проверки электронной подписи, Валидации, Подписания и Шифрования.

Администратор Удостоверяющего Центра — Лицо, уполномоченное приказом директора ООО «ОАС» осуществлять функции контроля и управления Автоматизированной системой Удостоверяющего Центра, в том числе, занесения информации о Юридических Лицах, контроля выпуска и аннулирования Сертификатов ключей проверки электронной подписи.

Администратор Юридического Лица — Лицо, уполномоченное единоличным исполнительным органом Юридического Лица осуществлять функции контроля и управления Автоматизированной системой Удостоверяющего Центра в части, ограниченной Сертификатами, выпускаемыми в отношении этого Юридического Лица, в том числе занесение информации о сотрудниках Юридического Лица, управлению их привилегиями в Системе Электронного Взаимодействия, перевыпуска, аннулирования и контроля выпущенных Сертификатов в отношении этого Юридического Лица.

Система Электронного Взаимодействия — автоматизированная система, создаваемая и поддерживаемая ООО «ОАС», с целью обеспечения прозрачного доступа к различным электронным ресурсам децентрализованной информационной системы ООО «ОАС», механизмов контроля и учета выдаваемых неисключительных лицензий на Программное Обеспечение, включая сроки действия таких лицензий и лицензируемое Оборудование, а также доступа Физических и Юридических Лиц в закрытые части информационной системы ООО «ОАС».

Пользователи Системы Электронного Взаимодействия — ЮЛ и ФЛ, являющиеся Владельцами Ключей ЭП в отношении которых УЦ «Исток» выпущен Сертификат.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЭП	Электронная подпись
ПЭП	Простая электронная подпись
УЭП	Усиленная неквалифицированная электронная подпись
УКЭП	Усиленная квалифицированная электронная подпись
Ключ ЭП	Ключ электронной подписи
КПЭП	Ключ проверки электронной подписи
УЦ	Удостоверяющий центр
СЭВ	Система электронного взаимодействия
ФЛ	Физическое лицо
ЮЛ	Юридическое лицо
ИП	Физическое лицо являющееся индивидуальным предпринимателем
ПО	Программное обеспечение
РАС	Реестр аннулированных Сертификатов
СКЗИ	Средства криптографической защиты информации
ПДн	Персональные данные

1 ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1 Настоящий регламент устанавливает порядок выпуска и обслуживания Головным и Подчиненными УЦ Сертификатов, и осуществления ООО «ОАС» иных функций, предусмотренных настоящим Регламентом, в рамках распределенной информационной системы ООО «ОАС».

1.2 Настоящий регламент применяется участниками СЭВ, использующими в своих отношениях УЭП для коммерческой деятельности.

1.3 Головной и Подчиненные Удостоверяющие Центры ООО «ОАС» создаются в целях контроля и проверки подлинности Сертификатов и Подписей, установленных с использованием таких Сертификатов.

1.4 Настоящий Регламент составляется в электронной форме, утверждается и заверяется УКЭП директора ОАО «ОАС».

1.5 Регламент и приказ о назначении администратора УЦ публикуются путем размещения в формате электронных документов на ресурсе Автоматизированной системы УЦ в сети «Интернет», доступном по адресу <https://cert.oas.su/about>.

1.6 Настоящий Регламент вступает в силу со дня его публикации в порядке, установленном п. 1.5 настоящего Реглаamenta.

1.7 Нормы, содержащиеся в Регламенте, становятся обязательными для пользователей услуг ООО «ОАС» с момента получения ими Сертификата.

1.8 Срок действия Реглаamenta – 1 год.

1.9 Если ООО «ОАС» не уведомит пользователей услуг УЦ о прекращении действия Реглаamenta, срок действия Реглаamenta автоматически пролонгируется на следующий год.

1.10 Уведомление Пользователей СЭВ происходит путем направления каждому Пользователю СЭВ соответствующего сообщения на адрес электронной почты.

1.11 ООО «ОАС» может вносить в одностороннем порядке изменения (дополнения) в текущую редакцию Реглаamenta, а также принимать изменения в форме издания новых редакций Реглаamenta.

1.12 Изменению не подлежат положения Реглаamenta, прямо или косвенно ущемляющие права пользователей услуг УЦ, за исключением случаев, когда такие изменения вносятся в соответствии с изменением законодательства Российской Федерации, либо изменениями международных регламентов по информационной безопасности в отношении СКЗИ.

1.13 Изменения (дополнения) Реглаamenta доводятся до сведения Пользователей СЭВ способом, установленным п. 1.10 настоящего Реглаamenta.

1.14 Изменения (дополнения) в Регламент вступают в силу на 5 (пятый) рабочий день со дня отправки Пользователям СЭВ уведомлений.

1.15 Все изменения (дополнения) в Регламент подлежат публикации в виде составе новой Редакции в порядке п. 1.5 настоящего Реглаamenta.

2 ФУНКЦИИ УЦ

2.1 Головной и Подчиненные УЦ ООО «ОАС» имеют ограниченный набор функций в зависимости от целей их создания, а также уровня подчиненности, и определяются настоящим Регламентом.

2.2 Все Удостоверяющие Центры ООО «ОАС», вне зависимости от целей их создания, осуществляют следующие функции:

2.2.1 Создают Сертификаты и выпускают их по запросу Владельцев Ключей ЭП.

2.2.2 Устанавливают сроки действия Сертификатов.

2.2.3 Ведут Реестр актуальных Сертификатов, выпущенных этим УЦ.

2.2.4 Аннулируют выпущенные этим УЦ Сертификаты.

2.2.5 Ведут Реестр аннулированных Сертификатов, выпущенных этим УЦ.

2.3 Головной УЦ ООО «ОАС» ограничивается выпуском Сертификатов подчиненных Удостоверяющих Центров и не может быть использован для выпуска иных Сертификатов с целями, отличными от «Удостоверяющий Центр», «Подписание Сертификатов» и «Подписание РАС».

2.4 Подчиненный УЦ «Исток» создается с целью обслуживания Сертификатов, выпускаемых Физическим и Юридическим лицам, а также Оборудованию, принадлежащему таким Лицам и дополнительно осуществляет следующие функции:

2.4.1 Устанавливает ограничения для Сертификатов ФЛ и ЮЛ для осуществления целей:

2.4.1.1 Подписание и Шифрование электронных документов.

2.4.1.2 Осуществление двусторонней аутентификации в СЭВ.

2.4.1.3 Авторизация уровня доступа к ресурсам распределенной информационной системы ООО «ОАС».

2.4.1.4 Использование механизмов Подписания и Шифрования электронной почты Владелец Ключа ЭП.

2.4.1.5 Подписание КПЭП

2.4.2 Устанавливает ограничения для Сертификатов Оборудования для осуществления целей:

2.4.2.1 Осуществление аутентификации узла сети (Сервера).

2.4.2.2 Осуществление шифрования передаваемых данных по каналам связи локальной и глобальной сети.

2.4.2.3 Осуществление двусторонней аутентификации и дальнейшей авторизации доступа к ресурсам распределенной информационной системы ООО «ОАС».

2.4.2.4 Подписание КПЭП

2.4.3 В случае заключения дополнительного соглашения между ЮЛ и ООО «ОАС» либо приобретения лицензии на ПО, реализующего функции корпоративного УЦ, может устанавливать ограничения для Сертификатов Оборудования для работы в качестве подчиненного УЦ, подчиняющегося непосредственно УЦ «Исток» с следующими целями:

2.4.3.1 Удостоверяющий Центр без права создания Подчиненных УЦ.

2.4.3.2 Подписание Сертификатов.

2.4.3.3 Подписание РАС.

2.4.3.4 Подписание КПЭП

2.4.4 Подчиненный УЦ, выпущенный УЦ «Исток», является собственностью ЮЛ, в отношении которого он был выпущен, но может быть отозван ООО «ОАС» в случаях нарушения настоящего Регламента, в том числе, компрометации Ключа ЭП Подчиненного УЦ.

2.4.5 Ответственность за Сертификаты, выпущенные Подчиненным УЦ, Сертификат которого выпущен УЦ «Исток», возлагается на Владельца Ключа ЭП, в отношении которого был выпущен Сертификат Подчиненного УЦ. Такое Лицо самостоятельно должно контролировать выпуск, аннулирование и сроки действия Сертификатов, выпущенных таким УЦ, включая обязательную публикацию РАС в публичной части корпоративного портала или сайта в сети «Интернет».

2.5 Подчиненный УЦ «Лицензирования» создается с целью обслуживания Сертификатов, выпускаемых Физическим и Юридическим лицам, в отношении которых были переданы неисключительные права пользования ПО или его частями для работы на определенном числе единиц Оборудования такого Лица и контроля сроков действия неисключительной лицензии на право пользования ПО или его частей.

2.5.1 УЦ «Лицензирования» ограничивает Сертификаты, выпущенные ПО или его частям в следующих целях:

2.5.1.1 Осуществление двусторонней аутентификации к ресурсам распределенной информационной системы ООО «ОАС».

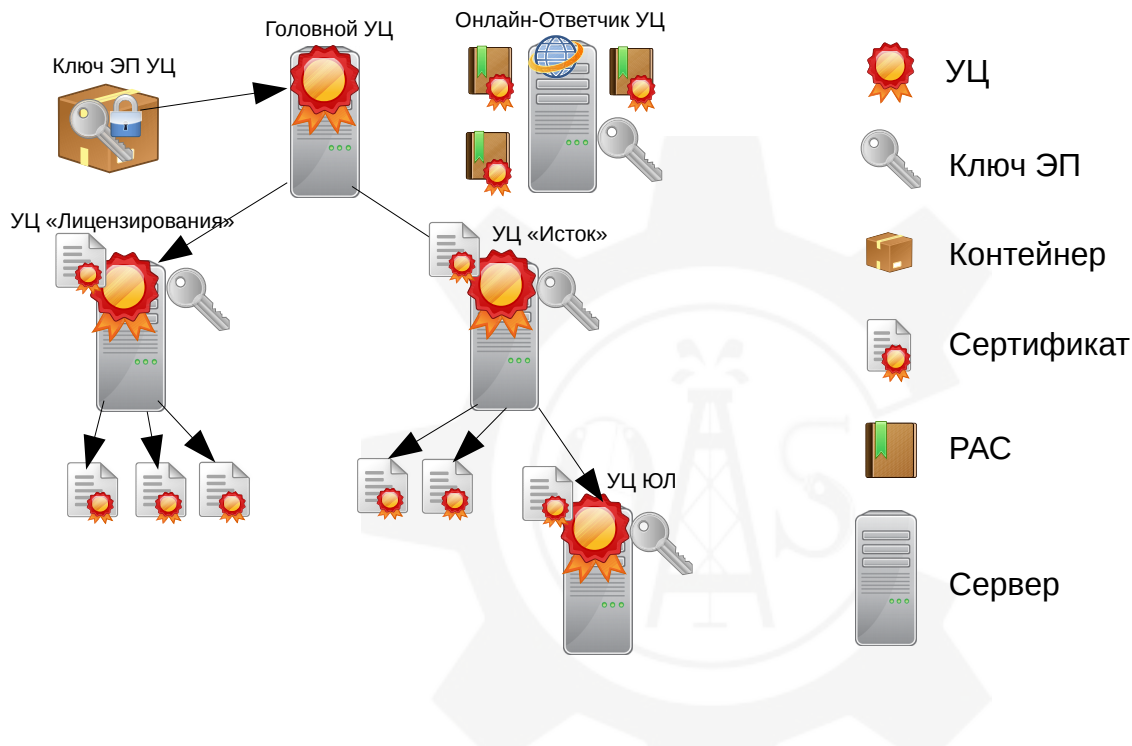
2.5.1.2 Подписание КПЭП.

2.5.2 УЦ «Лицензирования» ведет учет количества единиц Оборудования и серийные номера дисков, на которых функционирует Операционная Система, исполняющая лицензированную копию ПО.

2.5.3 ЮЛ или ИП, в отношении которых выпущены Сертификаты лицензируемого ПО или его частей, имеют доступ к ведомому УЦ «Лицензирования» Реестру активных Сертификатов в отношении этого Лица и имеют право отправить запрос на аннулирование Сертификата лицензируемого ПО или его части в рамках действующего Соглашения.

3 СТРУКТУРА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

3.1 Графическое представление УЦ (Цепочка УЦ)



3.2 Головной УЦ ООО «ОАС» является основным УЦ ООО «ОАС», для которого действует правило безоговорочного доверия к Ключу ЭП такого УЦ и который используется исключительно для выпуска Сертификатов Подчиненных УЦ. В целях обеспечения безопасности и защиты от компрометации УЦ используются следующие методы охраны Ключа ЭП:

3.2.1 Головной УЦ не является постоянно действующим УЦ ООО «ОАС» и задействуется только для целей выпуска и/или перевыпуска Сертификатов Подчиненных УЦ.

3.2.2 Ключ ЭП Головного УЦ хранится на внешнем накопителе в сейфе ООО «ОАС».

3.2.3 Ключ ЭП помещается в конверт, печатывается и подписывается директором ООО «ОАС».

3.2.4 Извлечение Ключа ЭП Головного УЦ из внешнего накопителя осуществляется отдельным приказом директора ООО «ОАС» о необходимости выпуска и/или перевыпуска Сертификатов Подчиненных УЦ.

3.2.5 Выпуск и/или перевыпуск Сертификатов Подчиненных УЦ осуществляется лично, либо под строгим контролем директора ООО «ОАС».

3.2.6 После выпуска новых Сертификатов Подчиненных УЦ, производится уничтожение всех копий Ключа ЭП Головного УЦ, если таковые создавались, и внешний накопитель с Ключем ЭП Головного УЦ печатывается и перемещается на хранение в сейф ООО «ОАС».

3.3 УЦ «Исток» является Подчиненным УЦ ООО «ОАС» первого уровня и может выпускать Сертификаты других Подчиненных УЦ, в порядке обусловленном настоящим Регламентом.

3.3.1 УЦ «Исток» выпускает Сертификаты для ЮЛ и ИП, подписавших Соглашение с ООО «ОАС».

3.3.2 УЦ «Исток» выпускает Сертификаты ФЛ, являющимися сотрудниками ЮЛ и сотрудниками ИП, подписавших Соглашение.

3.3.3 Запрещается осуществлять выпуск Сертификатов УЦ «Исток» в отношении Лиц, не являющихся Лицами, заключившими Соглашение, или сотрудниками таких Лиц.

3.3.4 В случаях, если Сертификат требуется Лицу, выполняющему работы по договору Гражданско-правового характера в интересах Лица, подписавшего Соглашение, Сертификат может быть выпущен на срок, не превышающий срока действия такого договора.

3.3.5 УЦ «Исток» выпускает Сертификаты, однозначно идентифицирующие аутентичность адреса Оборудования в корпоративной сети, в том числе с указанием принадлежности такого Оборудования ЮЛ или ИП, подписавшему Соглашение. Допускается продление таких Сертификатов в автоматическом режиме.

3.4 УЦ «Лицензирования» является Подчиненным УЦ ООО «ОАС» первого уровня и может выпускать Сертификаты ограниченного целевого назначения.

3.4.1 Сертификаты выпускаются с целью однозначной идентификации правомерности использования ПО или его части на единице Оборудования, принадлежащего ЮЛ или ИП.

3.4.2 Сертификаты ограничивают время использования такого ПО или его части сроком действия Сертификата, который устанавливается исходя из сроков действия неисключительного права пользования таким ПО или его частью.

3.4.3 Сертификаты могут быть отозваны в любой момент времени при подозрении в неправомерном использовании ПО или его части, в том числе при обнаружении факта такого использования.

3.4.4 Сертификаты могут быть продлены автоматически в срок за две недели до окончания срока действия Сертификата, если срок действия неисключительного права пользования ПО или его частью был продлен с момента выпуска Сертификата.

3.5 Публичный портал УЦ содержит сведения необходимые для осуществления работы инфраструктуры публичного ключа, соблюдения законодательства РФ и настоящего Регламента. На публичном портале УЦ размещаются следующие документы:

3.5.1 Текущая редакция настоящего регламента

3.5.2 Текст Соглашения к договорам Подписки или Технического сопровождения

3.5.3 Текст Соглашения к Дистрибьютерскому договору

3.5.4 Текст дополнительного Соглашения об обмене Реестрами актуальных Сертификатов

3.5.5 Сертификат Головного УЦ

3.5.6 РАС Головного УЦ

3.5.7 Сертификат УЦ «Исток»

3.5.8 РАС УЦ «Исток»

3.5.9 Сертификат УЦ «Лицензирования»

3.5.10 РАС УЦ «Лицензирования»

3.6 Публичный онлайн-ответчик УЦ хранит копию РАС и осуществляет проверку наличия запрашиваемого серийного номера Сертификата в РАС.

3.7 Публичный онлайн-ответчик УЦ подписывает ответ об отсутствии или присутствии серийного номера Сертификата в РАС, дату и причину такого аннулирования Сертификата собственным Ключем ЭП Сертификата онлайн-ответчика УЦ, выпущенным для целей работы онлайн-ответчика.

4 СВЕДЕНИЯ О ВЫПУСКАЕМЫХ СЕРТИФИКАТАХ

4.1 При организации работы Удостоверяющих Центров и Автоматизированной системы УЦ используются такие Средства Удостоверяющего Центра как:

4.1.1 Стандартная открытая платформенно-независимая библиотека OpenSSL под управлением ОС семейства GNU/Linux.

4.1.2 Модульная библиотека расширения Веб-сервера PHPSeclib, с использованием Веб-сервера Apache 2.4 защищенном реверсивным HTTPS прокси-сервером Nginx под управлением ОС семейства GNU/Linux.

4.1.3 Выпуск Сертификатов Автоматизированной системой УЦ с использованием HTML5 механизма WebCrypto API для поддерживаемых обозревателей Chromium Browser, Google Chrome, Mozilla Firefox, Opera, Safari, Microsoft Edge, Microsoft Internet Explorer актуальных версий на момент утверждения редакции настоящего Регламента.

4.2 Владельцами Ключей ЭП используются встроенные в операционную систему средства электронной подписи, совместимые со стандартном x509, и использующие алгоритм шифрования RSA, либо приобретаемые Владельцем ЭП в порядке, установленном разработчиком СКЗИ, если по каким-либо причинам использование встроенных средств электронной подписи является невозможным.

4.3 Рекомендуемым обозревателем для взаимодействия с Автоматизированной системой УЦ является Mozilla Firefox или его производные.

4.4 Используемым алгоритмом ЭП устанавливается стандартный алгоритм RSA с длиной ключа определяемой заявителем, но не менее чем 2048 бит, и не более 4096.

4.5 Сроки выпуска Сертификатов в зависимости от их целей устанавливаются УЦ следующим образом:

4.5.1 Головной УЦ — Бессрочно

4.5.2 Подчиненный УЦ — 10 лет

4.5.3 Подчиненный УЦ второго уровня — На весь срок действия Соглашения, но не более 5 лет

4.5.4 Сертификат ЮЛ, ФЛ — На весь срок действия Соглашения, но не более 1 года

4.5.5 Сертификат Оборудования — Бессрочно

4.5.6 Сертификат ПО — На весь срок действия неисключительного права пользования ПО или его частью, включая бессрочный выпуск таких Сертификатов

4.6 Общедоступными адресами в сети «Интернет» для целей доступа к сведениям, содержащимся в РАС и Сертификатам Удостоверяющих Центров устанавливаются следующие адреса для всех выпускаемых такими УЦ Сертификатов:

4.6.1 Сертификаты выпускаемые Головным УЦ содержат следующие адреса:

4.6.1.1 Сертификат УЦ: <https://cert.oas.su/public/ca.crt>

4.6.1.2 РАС УЦ: <https://cert.oas.su/public/ca.crl>

4.6.1.3 Онлайн-Ответчик УЦ: <https://cert.oas.su/ocsp>

4.6.2 Сертификаты выпускаемые УЦ «Исток» содержат следующие адреса:

4.6.2.1 Сертификат УЦ: <https://cert.oas.su/public/source-ca.crt>

4.6.2.2 РАС УЦ: <https://cert.oas.su/public/source-ca.crl>

4.6.2.3 Онлайн-Ответчик УЦ: <https://cert.oas.su/ocsp>

4.6.3 Сертификаты выпускаемые УЦ «Лицензирования» содержат следующие адреса:

4.6.3.1 Сертификат УЦ: <https://cert.oas.su/public/licensing-ca.crt>

4.6.3.2 РАС УЦ: <https://cert.oas.su/public/licensing-ca.crl>

4.6.3.3 Онлайн-Ответчик УЦ: <https://cert.oas.su/ocsp>

4.6.4 Сертификаты, выпускаемые Подчиненными УЦ, выпущенными УЦ «Исток» должны содержать адреса, необходимые для обеспечения проверки подлинности УЦ и загрузки РАС такого УЦ. Наличие Онлайн-Ответчика УЦ не является обязательным условием функционирования такого УЦ.

4.6.5 Сертификаты, выпускаемые Подчиненными УЦ, выпущенными УЦ «Исток» могут содержать в составе Сертификат выпустившего их УЦ с целью упрощения механизмов проверки выпущенных таким УЦ Сертификатов другими участниками СЭВ.

4.7 Субъекты выпускаемых Удостоверяющими Центрами Сертификатов содержат следующие поля, в зависимости от целей функционирования УЦ и типа выпускаемого сертификата:

4.7.1 Сертификат выпущенный в отношении ЮЛ содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ЮЛ
Регион/Область	2.5.4.8	Регион/Область регистрации ЮЛ
Почтовый индекс	2.5.4.17	Почтовый индекс ЮЛ
Адрес регистрации	2.5.4.9	Юридический адрес ЮЛ
Почтовый адрес	2.5.4.16	Почтовый адрес ЮЛ
Организация	2.5.4.10	Полное наименование ЮЛ
ОГРН	1.2.643.100.1	ОГРН ЮЛ
ИНН	1.2.643.3.131.1.1	ИНН ЮЛ
Полное имя	2.5.4.3	Полные ФИО единоличного исполнительного органа ЮЛ
Имя	2.5.4.41	Имя единоличного исполнительного органа ЮЛ
Фамилия	2.5.4.4	Фамилия единоличного исполнительного органа ЮЛ
Отчество	2.5.4.42	Отчество единоличного исполнительного органа ЮЛ
Электронная почта	1.2.840.113549.1.9.1	Адрес электронной почты ЮЛ
Должность	2.5.4.12	Директор
Роль	2.5.4.72	director

4.7.2 Сертификат, выпущенный в отношении ИП содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ИП
Регион/Область	2.5.4.8	Регион/Область регистрации ИП
Почтовый индекс	2.5.4.17	Почтовый индекс ИП
Адрес регистрации	2.5.4.9	Юридический адрес ИП
Почтовый адрес	2.5.4.16	Почтовый адрес ИП

Наименование поля	ОИД	Значение поля
Организация	2.5.4.10	ИП «Полные ФИО ИП»
ОГРНИП	1.2.643.100.5	ОГРНИП ИП
ИНН	1.2.643.3.131.1.1	ИНН ИП
Полное имя	2.5.4.3	Полные ФИО ИП
Имя	2.5.4.41	Имя ИП
Фамилия	2.5.4.4	Фамилия ИП
Отчество	2.5.4.42	Отчество ИП
Электронная почта	1.2.840.113549.1.9.1	Адрес электронной почты ИП
Должность	2.5.4.12	Индивидуальный Предприниматель
Роль	2.5.4.72	director

4.7.3 Сертификат, выпущенный в отношении ФЛ, являющегося сотрудником ЮЛ, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ЮЛ
Регион/Область	2.5.4.8	Регион/Область регистрации ЮЛ
Почтовый индекс	2.5.4.17	Почтовый индекс ЮЛ
Адрес регистрации	2.5.4.9	Юридический адрес ЮЛ
Почтовый адрес	2.5.4.16	Почтовый адрес ЮЛ
Организация	2.5.4.10	Полное наименование ЮЛ
ОГРН	1.2.643.100.1	ОГРН ЮЛ
ИНН	1.2.643.3.131.1.1	ИНН ЮЛ
Полное имя	2.5.4.3	Фамилия Имя сотрудника или ФИО сотрудника
Имя	2.5.4.41	Имя сотрудника
Фамилия	2.5.4.4	Фамилия сотрудника
Отчество	2.5.4.42	Дополнительное поле Отчество сотрудника
Электронная почта	1.2.840.113549.1.9.1	Адрес электронной почты сотрудника
Должность	2.5.4.12	Сотрудник или должность указанная работодателем
Роль	2.5.4.72	technician или user в зависимости от уровня доступа

4.7.4 Сертификат, выпущенный в отношении ФЛ, являющегося сотрудником ИП, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ИП
Регион/Область	2.5.4.8	Регион/Область регистрации ИП
Почтовый индекс	2.5.4.17	Почтовый индекс ИП
Адрес регистрации	2.5.4.9	Юридический адрес ИП
Почтовый адрес	2.5.4.16	Почтовый адрес ИП
Организация	2.5.4.10	ИП «Полные ФИО ИП»
ОГРНИП	1.2.643.100.5	ОГРНИП ИП
ИНН	1.2.643.3.131.1.1	ИНН ИП
Полное имя	2.5.4.3	Фамилия Имя сотрудника или ФИО сотрудника
Имя	2.5.4.41	Имя сотрудника
Фамилия	2.5.4.4	Фамилия сотрудника
Отчество	2.5.4.42	Дополнительное поле Отчество сотрудника
Электронная почта	1.2.840.113549.1.9.1	Адрес электронной почты сотрудника
Должность	2.5.4.12	Сотрудник или должность указанная работодателем
Роль	2.5.4.72	technician или user в зависимости от уровня доступа

4.7.5 Сертификат, выпущенный в отношении Оборудования, принадлежащему ЮЛ, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ЮЛ
Регион/Область	2.5.4.8	Регион/Область регистрации ЮЛ
Почтовый индекс	2.5.4.17	Почтовый индекс ЮЛ
Адрес регистрации	2.5.4.9	Юридический адрес ЮЛ
Почтовый адрес	2.5.4.16	Почтовый адрес ЮЛ
Организация	2.5.4.10	Полное наименование ЮЛ
ОГРН	1.2.643.100.1	ОГРН ЮЛ
ИНН	1.2.643.3.131.1.1	ИНН ЮЛ
Полное имя	2.5.4.3	Адрес оборудования в корпоративной сети
Серийный номер	2.5.4.5	Серийный номер диска или MAC сетевого адаптера

4.7.6 Сертификат, выпущенный в отношении Оборудования, принадлежащему ИП, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ИП
Регион/Область	2.5.4.8	Регион/Область регистрации ИП
Почтовый индекс	2.5.4.17	Почтовый индекс ИП
Адрес регистрации	2.5.4.9	Юридический адрес ИП
Почтовый адрес	2.5.4.16	Почтовый адрес ИП
Организация	2.5.4.10	ИП «Полные ФИО ИП»
ОГРНИП	1.2.643.100.5	ОГРНИП ИП
ИНН	1.2.643.3.131.1.1	ИНН ИП
Полное имя	2.5.4.3	Адрес оборудования в локальной сети
Серийный номер	2.5.4.5	Оборудование: адрес оборудования в локальной сети

4.7.7 Сертификат, выпущенный в отношении ПО или его части, неисключительное право пользования которым предоставлено на определенную единицу Оборудования ЮЛ, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ЮЛ
Регион/Область	2.5.4.8	Регион/Область регистрации ЮЛ
Почтовый индекс	2.5.4.17	Почтовый индекс ЮЛ
Адрес регистрации	2.5.4.9	Юридический адрес ЮЛ
Почтовый адрес	2.5.4.16	Почтовый адрес ЮЛ
Организация	2.5.4.10	Полное наименование ЮЛ
ОГРН	1.2.643.100.1	ОГРН ЮЛ
ИНН	1.2.643.3.131.1.1	ИНН ЮЛ
Полное имя	2.5.4.3	Наименование ПО или его части
Описание	2.5.4.13	Состав лицензируемого ПО и его описание
Имя	2.5.4.41	Кодовое наименование ПО или его части
Серийный номер	2.5.4.5	Серийный номер основного диска ОС

4.7.8 Сертификат, выпущенный в отношении ПО или его части, неисключительное право пользования которым предоставлено на определенную единицу Оборудования ИП, заключившим Соглашение содержит:

Наименование поля	ОИД	Значение поля
Страна	2.5.4.6	RU
Город	2.5.4.7	Город регистрации ИП
Регион/Область	2.5.4.8	Регион/Область регистрации ИП
Почтовый индекс	2.5.4.17	Почтовый индекс ИП
Адрес регистрации	2.5.4.9	Юридический адрес ИП
Почтовый адрес	2.5.4.16	Почтовый адрес ИП
Организация	2.5.4.10	ИП «Полные ФИО ИП»
ОГРНИП	1.2.643.100.5	ОГРНИП ИП
ИНН	1.2.643.3.131.1.1	ИНН ИП
Полное имя	2.5.4.3	Наименование ПО или его части
Описание	2.5.4.13	Состав лицензируемого ПО и его описание
Имя	2.5.4.41	Кодовое наименование ПО или его части
Серийный номер	2.5.4.5	Серийный номер основного диска ОС

4.8 ООО «ОАС», ровно как и Удостоверяющие Центры, не осуществляют хранение и обработку персональных данных и не является оператором персональных данных. Все сведения о ФЛ и ЮЛ, хранящиеся в базе данных Автоматизированной системы УЦ являются публичными сведениями ЕГРЮЛ/ЕГРИП и содержат обезличенные данные сотрудников такого Лица. Все дополнительные сведения, вносимые в Сертификат являются частью Сертификата и вносятся добровольно. Подписание документа Сертификатом с внесенными дополнительными полями эквивалентно добровольной публикацией дополнительных данных Сертификата, таких как «Отчество», «Область», «Город».

4.9 Ключ ЭП, соответствующий Сертификату, является конфиденциальной информацией Владельца Ключа ЭП. Удостоверяющий Центр не осуществляет создание и хранение Ключей ЭП, а также передачу их по каналам связи.

4.10 В случае прекращения деятельности УЦ все Сертификаты, выпущенные таким УЦ аннулируются.

5 ОБЩИЕ ПОЛОЖЕНИЯ О СЭВ

5.1 СЭВ является множеством электронных ресурсов, размещенных в распределенной информационной системе ООО «ОАС», включающей в себя такие ресурсы как:

- 5.1.1 Автоматизированная система УЦ
- 5.1.2 База знаний ООО «ОАС»
- 5.1.3 Репозиторий ПО и обновлений ПО ООО «ОАС»
- 5.1.4 Репозиторий ПО и обновлений ПО для ОС GNU/Linux Ubuntu
- 5.1.5 Репозиторий ПО и обновлений ПО для ОС GNU/Linux Mint
- 5.1.6 Личный кабинет ЮЛ и ФЛ
- 5.1.7 Личный кабинет лицензирования ПО
- 5.1.8 Дистрибьютерский личный кабинет

5.2 Доступ к СЭВ осуществляется с использованием защищенного шифрованного канала связи с опциональной аутентификацией по Сертификатам, выпущенным УЦ «Исток» и его Подчиненными УЦ.

5.3 Аутентификация узлов электронных ресурсов, размещенных в распределенной информационной системе ООО «ОАС», осуществляется с помощью Сертификатов, выпущенных внешним доверенным Головным УЦ, который не требует обязательного добавления в доверенные Головные УЦ применяемых в настоящее время ОС.

5.4 Основным протоколом доступа к СЭВ является протокол Hypertext Transport Protocol over Secure Socket Layers (HTTPS), и использует механизм Transport Layer Security (TLS) v1.2 с поддержкой Service Name Indication (SNI).

5.5 В случае, если при доступе к СЭВ не используется Сертификат, такой доступ считается публичным и предоставляется только в отношении публичной части СЭВ.

5.6 Запрещается передача и передоверие Ключа ЭП третьим лицам, в том числе нотариальное заверение на право использования Ключа ЭП.

5.7 Для целей передачи прав доступа к СЭВ должен осуществляться выпуск Сертификата в отношении Лица, которому осуществляется временная или постоянная передача таких прав с использованием Автоматизированной системы УЦ.

6 ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

6.1 Выпуск первичного Сертификата ФЛ и ЮЛ.

6.1.1 После заключения Соглашения, Администратор или иное уполномоченное Лицо, имеющее право управления Автоматизированной системой УЦ, заносит данные, необходимые для выпуска Сертификата, в том числе Идентификатор ПЭП, на портале Автоматизированной системы УЦ.

6.1.2 Автоматизированная система УЦ отправляет сообщение с использованием служб электронной почты с одноразовой ссылкой на выпуск Сертификата в адрес единоличного исполнительного Лица ЮЛ или ИП, используя Идентификатор ПЭП.

6.1.3 Лицо осуществляет обращение к Автоматизированной системе УЦ по переданной одноразовой ссылке и указывает дополнительные данные со своей стороны.

6.1.4 На стороне Лица формируется Ключ ЭП и КПЭП.

6.1.5 КПЭП и дополнительные данные передаются УЦ.

6.1.6 УЦ, используя Идентификатор ПЭП, дополнительные данные и КПЭП, создает запрос на Сертификат с указанием целей использования Сертификата и Подписывает его Ключем ЭП УЦ.

6.1.7 Выпущенный Сертификат отправляется Лицу Автоматизированной системой УЦ в формате PEM.

6.1.8 Сертификат устанавливается Лицом в локальное хранилище Сертификатов и сопоставляется с ранее сформированным Ключем ЭП.

6.2 Выпуск первичного Сертификата ПО и Оборудования

6.2.1 ПО или Оборудование формируют Ключ ЭП и КПЭП.

6.2.2 ПО или Оборудование создают запрос на Сертификат, исходя из конфигурации Оборудования.

6.2.3 Уполномоченное Лицо, владеющее Ключом ЭП соответствующего Сертификата доступа к СЭВ, получает ссылку на Автоматизированную систему УЦ от Оборудования или Программного Обеспечения для выпуска Сертификата ПО или Сертификата Оборудования.

6.2.4 Уполномоченное Лицо осуществляет обращение к Автоматизированной системе УЦ по переданной ссылке с Аутентификацией по личному Сертификату.

6.2.5 Автоматизированная система УЦ принимает переданный запрос на Сертификат ПО или Оборудования из ссылки и на основе информации, полученной из Субъекта Сертификата уполномоченного Лица, создает запрос на Сертификат ПО или Оборудования с указанием целей использования Сертификата, после чего передает его УЦ.

6.2.6 УЦ подписывает запрос, переданный Автоматизированной системой УЦ Ключем ЭП УЦ.

6.2.7 Выпущенный сертификат отправляется Лицу автоматизированной системой УЦ в формате PEM для последующей передачи ПО или Оборудованию.

6.2.8 Уполномоченное Лицо производит копирование содержимого Сертификата ПО или Оборудования в формате PEM в ПО или Оборудование, в отношении которого производился выпуск Сертификата.

6.3 Перевыпуск истекающего Сертификата ЮЛ или ФЛ.

6.3.1 За две недели до истечения срока действия Сертификата либо в случае изменения данных Субъекта, Владелец соответствующего Ключа ЭП должен обратиться в Автоматизированную систему УЦ для обновления такого Сертификата.

6.3.2 Владельцу Ключа ЭП необходимо изменить дополнительные данные, если они не соответствуют данным действующего Сертификата.

6.3.3 Новый Сертификат выпускается УЦ путем продления текущего Сертификата с последующей подписью Ключом ЭП УЦ при этом Ключ ЭП соответствующего Сертификата не изменяется.

6.4 Перевыпуск истекающего Сертификата ПО или Оборудования

6.4.1 Осуществляется автоматически

6.5 Перевыпуск истекшего или аннулированного Сертификата

6.5.1 Осуществляется в порядке, указанном в п.п. 6.1 и 6.2, за исключением случаев не требующих замены Ключа ЭП.

6.5.2 В случаях, не требующих замены Ключа ЭП, перевыпуск осуществляется с сохранением Ключа ЭП в порядке указанном в п.п. 6.1 и 6.2, КПЭП для создания нового Сертификата берется из текущего Сертификата.

6.6 Каждый выпускаемый или перевыпускаемый УЦ Сертификат имеет уникальный серийный номер Сертификата.

6.7 При выпуске или перевыпуске Сертификата в Реестр актуальных Сертификатов заносится серийный номер нового Сертификата со сбросом причины перевыпуска сертификата.

7 ПОРЯДОК АННУЛИРОВАНИЯ СЕРТИФИКАТОВ

7.1 Аннулирование Сертификатов производится Администратором УЦ или Администратором ЮЛ.

7.2 Сертификат должен быть аннулирован в случае смены занимаемой должности, изменении личных данных, адреса электронной почты и иных сведений, содержащихся в полях Субъекта Сертификата, с последующим перевыпуском Сертификата.

7.3 Сертификат должен быть аннулирован в случае увольнения сотрудника ЮЛ или ИП.

7.4 Сертификат должен быть аннулирован в иных случаях, предусмотренных Законами РФ или по решению Суда.

7.5 Для действующих Сертификатов, на этапе их перевыпуска производится запрос причины перевыпуска Сертификата в Реестре актуальных Сертификатов. Если причина перевыпуска Сертификата указана, происходит процедура аннулирования Сертификата.

7.6 Серийный номер аннулированного Сертификата вносится в РАС и РАС подписывается Ключем ЭП УЦ.

7.7 РАС публикуется на публичном портале УЦ и онлайн-ответчике УЦ.

8 ПОРЯДОК ВАЛИДАЦИИ СЕРТИФИКАТОВ КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

8.1 При получении Сертификата или электронного документа, подписанного с использованием Сертификата, СКЗИ осуществляет проверку полей Сертификата в следующем порядке:

8.1.1 Проверяется наличие УЦ, выпустившего Сертификат, в списке доверенных головных удостоверяющих центров, а в случае цепочки УЦ — вышестоящего УЦ, вплоть до головного УЦ в списке доверенных головных УЦ.

8.1.2 В случае требования протоколом передачи данных проверяется принадлежность Субъекта уникальному Идентификатору средства передачи данных, такому как, ПЭП или адресу Оборудования, в отношении которого был выпущен Сертификат.

8.1.3 Проверяется дата начала срока действия Сертификата на дату, находящуюся в прошлом или настоящем времени.

8.1.4 Проверяется дата окончания срока действия Сертификата на дату, находящуюся в настоящем или будущем времени.

8.1.5 Проверяются ограничения использования Сертификата в области, ограниченной целями выпуска Сертификата, применимо к текущему использованию Сертификата

8.1.6 Проверяется статус аннулирования Сертификата путем обращения к онлайн-ответчику УЦ, адрес которого указывается в расширении ключа AIA, с использованием серийного номера Сертификата, а в случае невозможности, загружается PAC с УЦ по адресу, который указывается в расширении ключа CRL, и проверяется отсутствие серийного номера Сертификата в загруженном PAC. При этом для PAC действуют такие же правила проверки Сертификата подписи PAC, как и для других электронных документов, подписанных Сертификатом.

8.1.7 Проверяется соответствие документа Подписи, установленной с использованием Сертификата.

8.2 В случае нарушения любого из условий проверки Сертификата, такой Сертификат считается не действительным, пользователь СКЗИ уведомляется о недействительности Сертификата или нарушения целостности электронного документа. Доступ к документу ограничивается, при этом, в случае необходимости, документ может быть прочитан, но не имеет юридической силы.

9 Компрометация Ключа ЭП

9.1 Владелец Ключа ЭП самостоятельно принимает решение о факте или угрозе Компрометации своего Ключа ЭП.

9.2 К событиям, относящимся к явной Компрометации Ключа ЭП, относятся:

9.2.1 Утрата Ключа ЭП и (или) оборудования, содержащего Ключ ЭП, в том числе с последующим его обнаружением;

9.2.2 Обнаружение нарушения правил хранения Ключа ЭП;

9.2.3 Доступ посторонних лиц в силу нотариального заверения прав Лица на осуществление действий от имени Владельца Ключа ЭП;

9.2.4 Доступ, в том числе временный, посторонних лиц к файлу, содержащему Ключ ЭП, или к информации о пароле для защиты такого файла;

9.2.5 Иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности доступа третьих лиц к файлу, содержащему Ключ ЭП, или паролю для защиты Ключа ЭП, в том числе передача файла с Ключом ЭП или его пароля по незащищенным каналам связи.

9.3 К событиям неявной Компрометации Ключа ЭП могут быть отнесены следующие подозрения:

9.3.1 Возникновение подозрений на утечку информации или ее искажение на оборудовании, содержащем Ключ ЭП (например, в случае обнаружения вирусного заражения средствами антивирусной защиты, установки нелегального программного обеспечения и т.д.);

9.3.2 Нарушение печати на сейфе, хранилище, содержащего Ключ ЭП;

9.3.3 Доступ третьих лиц к оборудованию, содержащему Ключ ЭП;

9.3.4 Другие случаи, когда нельзя достоверно установить, что произошло с Ключом ЭП (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута

возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц).

9.4 В случае Компрометации или угрозы Компрометации Ключа ЭП, Владелец Ключа ЭП прекращает его использование, обращается к Администратору ЮЛ или Администратору УЦ с уведомлением о случае Компрометации Ключа ЭП или угрозе Компрометации Ключа ЭП.

9.5 В случае выявления обстоятельств, которые могут свидетельствовать о наступлении событий, отнесенных к явной и/или неявной компрометации Ключа ЭП, Администратор ЮЛ или Администратор УЦ вправе аннулировать Сертификат, соответствующий скомпрометированному Ключу ЭП.

9.6 Случай Компрометации Ключа ЭП или подозрение в возможности Компрометации Ключа ЭП означают перевыпуск Сертификата, соответствующего скомпрометированному Ключу ЭП с созданием нового Ключа ЭП.

9.7 В случае Компрометации Ключа ЭП Головного УЦ, действие Головного УЦ и всех подчиненных УЦ приостанавливается до выпуска нового Ключа ЭП Головного УЦ и соответствующего ему Сертификата Головного УЦ, и перевыпуска всех связанных с ним Сертификатов, не затрагивая действующие Ключи ЭП.

9.8 В случае Компрометации Ключа ЭП Подчиненного УЦ, действие такого Подчиненного УЦ и всех его подчиненных УЦ приостанавливается до выпуска нового Ключа ЭП Подчиненного УЦ и соответствующего ему Сертификата Подчиненного УЦ, и перевыпуска всех связанных с ним Сертификатов, не затрагивая действующие Ключи ЭП.

9.9 В случае Компрометации Ключа ЭП и последующего аннулирования Сертификата соответствующего скомпрометированному Ключу ЭП, такой Сертификат считается действительным до фактической даты аннулирования Сертификата.

9.10 УЦ помещает аннулированный Сертификат в соответствующий РАС с указанием причины «Компрометация ключа».

10 ПРАВООТНОШЕНИЯ УСТАНОВЛИВАЕМЫЕ НАСТОЯЩИМ РЕГЛАМЕНТОМ

10.1 ООО «ОАС» имеет право:

10.1.1 Проверять сведения, указанные при заключении Соглашения, указываемые в Сертификатах ЮЛ или ИП, на соответствие данным указанным в ЕГРЮЛ/ЕГРИП и наличие инициированной процедуры банкротства или ликвидации таких Лиц.

10.1.2 Отказать в выпуске Сертификатов ЮЛ или ФЛ в случае нарушения настоящего Регламента.

10.1.3 Аннулировать существующие Сертификаты ЮЛ, ФЛ, Оборудования или ПО в случае компрометации Ключа ЭП, соответствующего такому Сертификату или нарушении настоящего Регламента.

10.2 ООО «ОАС» обязано:

10.2.1 Опубликовать настоящий Регламент на публичном портале УЦ.

10.2.2 Создавать Сертификаты по запросам ФЛ и ЮЛ, заключившим Соглашение с ООО «ОАС».

10.2.3 Аннулировать Сертификаты по обращению Владельцев Ключей ЭП соответствующих таким Сертификатам.

10.2.4 Вести Реестр актуальных Сертификатов, обеспечивать его актуальность и доступ к нему ФЛ и ЮЛ заключивших Соглашение.

10.2.5 Вести РАС, обеспечивать его актуальность и публичный доступ к нему на публичном портале УЦ.

10.2.6 Обеспечивать уникальность серийных номеров в выпускаемых УЦ ООО «ОАС» Сертификатах.

10.2.7 Осуществлять по обращению пользователей СКЗИ подтверждение подлинности Сертификата и Подписи, установленной с использованием такого Сертификата, в отношении выпущенных УЦ ООО «ОАС» Сертификатов.

10.3 Администратор УЦ обязан:

10.3.1 Аннулировать Сертификат при поступлении уведомления о компрометации соответствующего Ключа ЭП.

10.3.2 Выполнять требования вышестоящего руководства.

10.3.3 Организовывать техническое обслуживание вычислительной техники, используемой для целей функционирования инфраструктуры УЦ.

10.3.4 Выполнять требования по защите информации ограниченного распространения.

10.3.5 Не разглашать сведения, ставшие ему известными, в связи с исполнением его должностных обязанностей.

10.4 Пользователи СЭВ имеют право:

10.4.1 Обращаться в УЦ с запросом на выпуск нового Сертификата.

10.4.2 Обращаться в УЦ с запросом об аннулировании действующего Сертификата, соответствующего Ключу ЭП, владельцем которого является заявитель.

10.4.3 Вносить дополнительные сведения в выпускаемые УЦ Сертификаты.

10.4.4 Обращаться в УЦ с целью проверки отсутствия серийного номера Сертификата, выпущенного таким УЦ в РАС.

10.4.5 Обращаться в УЦ с целью получения РАС.

10.4.6 Получать сведения из Реестра актуальных Сертификатов в отношении Физических Лиц, являющихся сотрудниками ЮЛ и ИП, заключившими дополнительное Соглашение об обмене Реестрами актуальных Сертификатов.

10.5 Пользователи СЭВ обязаны:

10.5.1 Выразить согласие с положениями настоящего Регламента и следовать ему.

10.5.2 Обеспечивать сохранение в тайне своих Ключей ЭП и применять все возможные меры для предотвращения компрометации и утери таких Ключей ЭП.

10.5.3 Использовать Сертификаты только для целей, разрешенных соответствующими расширениями Сертификата.

10.5.4 Немедленно уведомлять о возможной компрометации Ключа ЭП вышестоящее руководство или аннулировать Сертификаты соответствующие скомпрометированному Ключу ЭП с использованием Автоматизированной системы УЦ.

11 ПОРЯДОК РАЗРЕШЕНИЯ РАЗНОГЛАСИЙ

11.1 Применение УЭП в СЭВ может приводить к конфликтным ситуациям, заключающимся в оспаривании Пользователями СЭВ авторства и/или содержимого документа, подписанного УЭП.

11.2 Разбор конфликтной ситуации заключается в доказательстве подлинности УЭП конкретным Пользователем СЭВ под конкретным электронным документом.

11.3 Данный разбор основывается на математических свойствах алгоритма УЭП, реализованного в соответствии со стандартом RSA, гарантирующими невозможность подделки значения УЭП любым лицом, не обладающим Ключом ЭП и не имеющим специальных технических средств для подбора такого Ключа ЭП.

11.4 Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон и уполномоченных лиц УЦ.

11.5 ООО «ОАС» принимает во внимание, что ни один алгоритм генерации Ключа ЭП, вне зависимости от длины Ключа ЭП не может обеспечить гарантированной защиты Ключа ЭП, в том числе от способов полного перебора Ключей ЭП с использованием специального криптографического оборудования, компрометации Ключа ЭП, социального инженеринга и других способов получения доступа к Ключу ЭП. Все подобные возможности должны рассматриваться и оцениваться комиссией по разбору конфликтных ситуаций.

11.6 Разбор конфликтной ситуации выполняется по инициативе любого участника автоматизированной системы и состоит из:

11.6.1 Предъявления претензии одной стороны другой.

11.6.2 Формирования комиссии.

11.6.3 Разбора конфликтной ситуации.

11.6.4 Принятия решения.

11.7 Разбор конфликтной ситуации проводится с использованием различных СКЗИ общего назначения, в том числе на гарантированно не скомпрометированном оборудовании, для электронного документа, авторство или содержание которого оспаривается.

11.8 Проверка подписанного электронного документа включает в себя выполнение следующих действий:

11.8.1 Определение Сертификата, необходимого для проверки УЭП.

11.8.2 Проверка УЭП электронного документа с использованием Сертификата.

11.8.3 Проверка подлинности УЭП УЦ, выпустившего Сертификат.

11.8.4 Проверка действительности Сертификата на момент времени, указанный предъявляющей претензии стороной.

11.8.5 Проверка действительности Сертификата на момент времени, указанного в УЭП электронного документа.

11.8.6 Проверка отсутствия сертификатов ключей проверки электронной подписи в списке аннулированных сертификатов на момент времени, указанный предъявляющей претензии стороной.

11.9 Протокол проверки УЭП, является основным документом работы комиссии и должен быть подписан всеми членами комиссии.

11.10 При положительном результате проверки УЭП документа, Верификации Сертификата, отсутствии серийного номера Сертификата в РАС, авторство подписи под документом считается установленным.

12 ОТВЕТСТВЕННОСТЬ

12.1 ООО «ОАС» несет ответственность за убытки при использовании Сертификата Владелец Ключа ЭП, соответствующего такому Сертификату, только в случае, если данные убытки возникли при Компрометации Ключей ЭП Головного и/или Подчиненных УЦ.

12.2 ООО «ОАС» не несет ответственности в случае нарушения Владелец ЭП положений настоящего Регламента, в том числе:

12.2.1 Неисполнения или несвоевременного исполнения обязательств по аннулированию Сертификатов, которые были выпущены на основании скомпрометированных Ключей ЭП.

12.2.2 Отсутствие обеспечения защиты от несанкционированного использования Ключей ЭП третьими лицами, повлекшими за собой компрометацию Ключа ЭП.

12.3 В ситуации, оговоренной п. 12.2 настоящего Регламента, претензии Владельца Ключа ЭП к ООО «ОАС» ограничиваются указанием на несоответствие его действий настоящему Регламенту.

12.4 Ответственность, предусмотренная главой 12 настоящего Регламента, ограничивается пределами сумм доказанного реального ущерба, причиненного Участнику СЭВ невыполнением или не

надлежащим выполнением обязательств другим Участником СЭВ. Ни один из Участников СЭВ не отвечает за неполученные доходы (упущенную выгоду), которые бы получил другой Участник СЭВ.

13 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

13.1 Положения настоящего Регламента должны рассматриваться в соответствии с нормативными документами по информационной безопасности и законами Российской Федерации.

13.2 Любые разногласия в отношении управления ключами и сертификатами должны разрешаться посредством соответствующего механизма урегулирования споров. По возможности разногласия должны разрешаться путем совместных переговоров. В случаях когда договоренность не достигается, спорная ситуация разрешается в судебном порядке в соответствии с законодательством Российской Федерации.

