Утвержден

Приказом АО «СИГНАЛ-КОМ»

от 02 февраля 2021 г. № 9

Удостоверяющий центр «e-Notary». Регламент

Москва

2021г.

Оглавление

1. Общие положения 5
1.1. Термины и определения 5
1.2. Сведения об Удостоверяющем центре «e-Notary» 9
1.3. Общие сведения о Регламенте 10
1.3.1. Статус регламента 11
1.3.2. Идентификация Регламента 11
1.3.3. Присоединение к Регламенту 11
1.3.4. Публикации Регламента и его изменений 11
1.3.5. Срок действия Регламента 12
1.3.6. Разрешение споров 12
1.3.7. Порядок расторжения Регламента 13
1.3.8. Применение регламента 13
1.4. Оплата услуг Удостоверяющего центра. Сроки и порядок расчетов 13
1.5. Финансовая ответственность 15
1.6. Прекращение деятельности Удостоверяющего центра 15
1.7. Контактная информация 15
2. Положения об удостоверяющем центре 16
2.1. Инфраструктура УЦ e-Notary 16
2.1.1. Удостоверяющий центр. Перечень функций и услуг 16
2.1.2. Регистрационные центры. Перечень функций и услуг 17
2.1.3. Справочник сертификатов 18
2.1.4. Web-интерфейс УЦ 19
2.2. Пользователи УЦ 19
2.3. Разновидности сертификатов и области их применения 19
2.3.1. Виды сертификатов 19
2.3.2. Сведения и документы, необходимые для изготовления сертификатов 20
2.3.3. Разрешенные области применения сертификатов 20
2.4. Права Удостоверяющего центра и Пользователя УЦ 20
2.4.1. Права УЦ e-Notary 20
2.4.2. Права Пользователей УЦ 22
2.4.3. Права Владельцев сертификатов 22
2.5. Обязанности Удостоверяющего центра и Пользователей УЦ 22
2.5.1. Обязанности Удостоверяющего центра 22
2.5.2. Обязанности заявителей 24
2.5.3. Обязанности владельцев сертификатов 25
2.6. Ответственность Удостоверяющего центра и Пользователей УЦ 25
2.6.1. Ответственность Удостоверяющего центра 25

2.6.2. Ответственность Владельцев сертификатов 26
2.7. Политика конфиденциальности 26
2.8. Идентификация и аутентификация 27
2.8.1. Система именования. Уникальность имен 27
2.8.2. Первичная идентификация и аутентификация Пользователя УЦ 27
2.8.3. Идентификация и аутентификация зарегистрированного Пользователя УЦ 28
3. Порядок и сроки предоставления услуг Удостоверяющим центром 29
3.1. Порядок действий при первичной регистрации Пользователей УЦ, генерации ключей и изготовления сертификатов 29
3.1.1. Порядок подачи документов на изготовление и выдачу сертификатов 29
3.1.2. Процедура генерации ключей ЭП и запросов на сертификаты 33
3.1.3. Порядок изготовления и выдачи сертификата при личном обращении Заявителя 35
3.2. Порядок действий при проведении плановой смены ключей ЭП и обновлении сертификатов Пользователей УЦ 37
3.3. Внеплановая смена ключей зарегистрированного Пользователя УЦ 38
3.5. Аннулирование (отзыв) сертификата Пользователя УЦ 38
3.5.1. Основания для прекращения действия или аннулирования сертификата Пользователя УЦ 38
3.5.2. Порядок действия УЦ при аннулировании (отзыве) сертификата Пользователя УЦ 39
3.5.3. Порядок действий Пользователя УЦ при компрометации ключей ЭП 40
3.6. Порядок действий при смене ключей ЭП Удостоверяющего Центра 40
3.6.1. Плановая смена ключей ЭП Удостоверяющего центра 40
3.6.2. Компрометация ключей ЭП Удостоверяющего центра 41
3.7. Смена ключей оператора Регистрационного центра 41
3.7.1. Плановая смена ключей Оператора Регистрационного центра 42
3.7.2. Компрометации ключевых документов Оператора Регистрационного центра 42
3.8. Процедура подтверждения электронной подписи с использованием сертификата ключа проверки ЭП 42
3.9. Порядок ведения реестра квалифицированных сертификатов (Справочника сертификатов) 43
3.10. Порядок обслуживания реестра квалифицированных сертификатов (Справочника сертификатов) 44
4. Порядок исполнения обязанностей Удостоверяющего центра 44
4.1. Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки 44
4.2. Выдача по обращению Заявителя средств электронной подписи 44
4.3. Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий 45
4.4. Обеспечение доступности Спровочника сертификатов в информационно-телекоммуникационной сети «Интернет» 45

4.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей 45
4.6. Регистрация квалифицированного сертификата в Единой системе идентификации и аутентификации 46
4.7. Регистрация владельца квалифицированного сертификата в Единой системе идентификации и аутентификации 46
4.8. Предоставление доступа к информации, содержащейся в реестре квалифицированных сертификатов 46
5. Дополнительные положения 46
5.1. Требования к средствам электронной подписи Пользователей УЦ 46
5.2. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП 47
5.4. Копия сертификата ключа проверки ЭП в электронной форме 48
5.5. Копия сертификата ключа проверки ЭП на бумажном носителе 48
5.6. Архивное хранение документированной информации 49
5.6.1. Состав архивных документов 49
5.6.2. Комплектование архивного фонда 49
5.6.3. Архивное хранилище 49
5.6.4. Срок архивного хранения 49
5.6.5. Хранение сертификатов ключей подписей в Удостоверяющем центре 49
5.6.6. Уничтожение архивных документов 50
6. Структуры сертификатов и списка отозванных сертификатов 50
6.1. Структура сертификатов ключей проверки ЭП, формируемых Удостоверяющим центром 50
6.1.1. Базовые поля сертификата ключа проверки ЭП 50
6.1.2. Расширения сертификата ключа проверки ЭП 50
6.1.3. Объектные идентификаторы алгоритмов 51
6.1.4. Формы имени 51
6.1.5. Атрибуты имени 51
6.2. Структура СОС, формируемого Удостоверяющим Центром 52
6.2.1. Базовые поля СОС 52
6.2.2. Расширения СОС 53
6.2.3. Расширения записей списка аннулированных (отозванных) сертификатов 53
7. Рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ 54
Приложения 56

Общие положения

1.1. Термины и определения

Администратор Удостоверяющего центра (Администратор УЦ) – уполномоченный представитель Удостоверяющего центра, ответственный за выполнение операций по изготовлению и обслуживанию сертификатов ключей проверки электронной подписи Пользователей УЦ.

Аккредитованный удостоверяющий центр (аккредитованный УЦ) – Удостоверяющий центр, в отношении которого уполномоченным федеральным органом установлено его соответствие требованиям Федерального закона от 06.04.2011 г. №63-ФЗ «Об электронной подписи».

Аутентификация – гарантированное установление подлинности физического лица или организации, выступающих под некоторым именем и запрашивающих доступ к тому или иному ресурсу.

Владелец сертификата ключа проверки ЭП – лицо, которому в порядке, установленном Федеральным законом от 06.04.2011г. № 63-ФЗ «Об электронной подписи», Удостоверяющим центром выдан сертификат ключа проверки ЭП и которое владеет соответствующим ключом ЭП.

Запрос сертификата — электронный документ, содержащий ключ проверки ЭП с параметрами алгоритма, сведения о Владельце сертификата ключа проверки ЭП и некоторые дополнительные данные, заверенные электронной подписью Владельца.

Защищенный сервис – системы защищенного взаимодействия на базе PKI, имеющие различное прикладное назначение.

Заявитель — лицо, обратившееся в Удостоверяющий центр за получением сертификата ключа проверки ЭП.

Идентификация – процедура присвоения субъектам и объектам доступа некоторого идентификатора и/или сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов. Процедура идентификации сводится (1) к установлению факта соответствия заданного имени и реально существующего субъекта (физического лица или организации) и (2) к установлению факта, что субъект, запрашивающий доступ к ресурсам под заданным именем, является именно тем субъектом, которому заданное имя было присвоено в результате легальной процедуры.

Информационная система общего пользования – информационной система, участники электронного взаимодействия в которой составляют неопределенный круг лиц и в использовании которой этим лицам не может быть отказано.

Квалифицированный сертификат ключа проверки электронной подписи (квалифицированный сертификат) — сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган), и являющийся в связи с этим официальным документом;.

Ключевая фраза (Аварийный пароль) — пароль для экстренной связи Владельца сертификата ключа проверки ЭП с Администратором Удостоверяющего центра, используемый Владельцем для оповещения Администратора о компрометации своего ключа ЭП.

Ключ проверки электронной подписи (ключ проверки ЭП) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее — проверка электронной подписи).

Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Компрометация ключа ЭП – утрата доверия к тому, что используемый ключ ЭП обеспечивает безопасность информации; констатация Владельцем сертификата ключа проверки ЭП обстоятельств, при которых возможно несанкционированное использование его ключа ЭП неуполномоченными лицами.

Конфиденциальность информации – субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Корпоративная информационная система – информационной система, участники электронного взаимодействия в которой составляют определенный круг лиц.

Копия сертификата ключа проверки электронной подписи – документ на бумажном носителе, содержащий информацию из сертификата ключа проверки ЭП, заверенную собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра.

Криптографическая защита — защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

Криптографические ключи – общее название открытых и закрытых (секретных) ключей:

- закрытый (секретный) ключ – уникальная последовательность символов, известная Подписчику сертификата соответствующего открытого ключа и предназначенная для создания электронной подписи и расшифрования информации с использованием криптографических средств;
- открытый ключ — уникальная последовательность символов, соответствующая закрытому (секретному) ключу, доступная Пользователям сертификатов и предназначенная для подтверждения подлинности электронной подписи и зашифрования информации с использованием криптографических средств.

Оператор Регистрационного центра (Оператор РЦ) — уполномоченный представитель Регистрационного центра, ответственный за выполнение операций по идентификации, аутентификации, проверке полномочий заявителей, претендующих на получение сертификата, и передаче сформированных ими запросов сертификатов Администратору УЦ.

Организатор – акционерное общество «СИГНАЛ-КОМ» — организатор Удостоверяющего центра e-Notary.

Плановая смена ключей — регламентируемая Администратором УЦ периодическая смена ключей электронной подписи УЦ, Операторов РЦ и Владельцев сертификатов, не вызванная их компрометацией.

Пользователь сертификата — физическое лицо, использующее полученные в Удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной подписи Владельцу сертификата ключа проверки ЭП.

Пользователь Удостоверяющего центра (далее — Пользователь) — физическое лицо, присоединившееся к Регламенту и использующее сертифицированный в удостоверяющем центре ключ ЭП для подписи электронных документов или сертификаты ключей проверки ЭП для проверки подписанных электронных документов (в случае присоединения к Регламенту юридического лица — физическое лицо, являющееся уполномоченным представителем юридического лица).

Портал Удостоверяющего центра e-Notary (Портал УЦ) — информационный Web-ресурс УЦ e-Notary, содержащий всю необходимую информацию об Удостоверяющем центре и оказываемых им услугах; на Портале УЦ расположен Интернет-магазин, через который пользователи могут заказать сертификаты и программное обеспечение, необходимое для формирование ключей и запросов на сертификаты.

Реестр Удостоверяющего центра – набор документов Удостоверяющего центра в электронной и/или бумажной форме, включающий следующую информацию:

- заявления о присоединении к Регламенту Удостоверяющего центра;
- регистрационные данные Пользователей Удостоверяющего центра;
- заявления на изготовление сертификата ЭП;
- заявления на аннулирование (отзыв) сертификата ЭП;
- заявления на приостановление/возобновление действия сертификата ЭП;
- сертификаты ключей проверки электронной подписи;
- списки отозванных сертификатов.

Регистрационный центр (РЦ) – опциональный субъект PKI, отвечающий за идентификацию, аутентификацию и проверку полномочий заявителей, претендующих на получение сертификата, но не подписывающий и не выпускающий сертификаты; обладает необходимым комплексом программно-технических средств электронной подписи и шифрования для организации защищенного канала связи, обеспечивающего достоверную передачу запросов сертификатов в УЦ.

Регламент – порядок реализации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей. Основной руководящий документ УЦ, отражающий обязанности Пользователей УЦ и членов группы администраторов, протоколы работы, принятые форматы данных, а также основные организационно-технические мероприятия, необходимые для безопасного функционирования УЦ.

Руководитель Удостоверяющего центра – сотрудник УЦ, обеспечивающий контроль за деятельностью Удостоверяющего центра, в том числе за обслуживающим персоналом, в целях соблюдения установленных правил работы в Удостоверяющем центре.

Самоподписанный запрос сертификата (формата PKCS#10) – запрос сертификата, подписанный ключом ЭП, парным ключу проверки ЭП, включенному в запрос.

Сертификат ключа проверки электронной подписи (сертификат ключа проверки ЭП, сертификат) – электронный документ или документ на бумажном носителе, выданные Удостоверяющим центром либо доверенным лицом Удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП Владельцу сертификата ключа проверки ЭП; включает в себя ключ проверки ЭП, информацию о Владельце сертификата, сведения об УЦ, выдавшем

сертификат, дополнительные атрибуты (расширения), определяемые требованиями использования сертификата ключа проверки ЭП в защищенной системе и др.

Сертификат УЦ (в иерархической модели построения УЦ) – сертификат ключа проверки ЭП одного УЦ, выпущенный другим УЦ, или «самозаверенный» сертификат корневого (root) УЦ.

Список отозванных (аннулированных) сертификатов (СОС) — электронный документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов ключей ЭП, которые на определенный момент времени были аннулированы (отозваны).

Средство криптографической защиты информации (СКЗИ) — в контексте данного документа — СКЗИ «Крипто-КОМ 3.3» (сертификаты соответствия ФСБ России №№ СФ/114-3615, СФ/124-3616 от 29.12.2018 г. для исполнений 7 и 8, соответственно), СКЗИ «Крипто-КОМ 3.4» (сертификаты соответствия ФСБ России №№ СФ/114-3975, СФ/124-3976 от 11.01.2021 г. для исполнений 42 и 43, соответственно), СКЗИ «CADB 2.1» (сертификаты соответствия ФСБ России №№ СФ/114-3755, СФ/124-3756 от 18.09.2019 г. для исполнений 1 и 2, соответственно) и СКЗИ «Signal-COM JCP 3.1» (сертификаты соответствия ФСБ России №№ СФ/114-3753, СФ/124-3754 от 18.09.2019 г. для исполнений 1 и 2, соответственно).

Средства электронной подписи (средства ЭП) — шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций — создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Средства Удостоверяющего центра (средства УЦ) — программные и (или) аппаратные средства, используемые для реализации функций Удостоверяющего центра.

Удостоверяющий центр (УЦ) – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом РФ от 06.04.2011г. №63-ФЗ «Об электронной подписи».

Удостоверяющий центр «e-Notary» (УЦ «e-Notary») – акционерное общество (АО) «СИГНАЛ-КОМ», реализующее целевые функции Удостоверяющего центра, именуемого «e-Notary», в соответствии с Федеральным законом Российской Федерации от 06.04.2011 г. №63-ФЗ «Об электронной подписи». Наличие государственной аккредитации Министерства связи и массовых коммуникаций Российской Федерации (Рег.№ 730 от 10.07.2017 г.) дает УЦ «e-Notary» право на изготовление и обслуживание квалифицированных сертификатов ключей проверки электронной подписи.

Уникальное имя (Distinguished Name в терминологии X.509) – набор атрибутов, совокупность которых, будучи включенной в сертификат, однозначно идентифицирует Владельца сертификата.

Уполномоченное лицо Удостоверяющего центра (Уполномоченное лицо УЦ) – сотрудник УЦ, отвечающий за формирование, хранение, эксплуатацию, обновление и уничтожение ключа ЭП и сертификата ключа проверки ЭП Удостоверяющего центра.

Уполномоченный представитель Заявителя, обратившегося за получением сертификата – физическое лицо (в том числе, сотрудник юридического лица), уполномоченное лицом стороны, присоединившейся к Регламенту, совершать от его имени действия, установленные для Пользователя УЦ в рамках Регламента.

Участник PKI – общее название Владельцев и Пользователей сертификатов.

Шифрование информации (шифрование) — взаимнооднозначное математическое (криптографическое) преобразование информации, зависящее от ключа (секретный параметр преобразования), которое ставит в соответствие блоку открытой информации блок зашифрованной информации.

Электронная подпись (ЭП) — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. Видами электронных подписей, отношения в области использования которых регулируются Федеральным законом РФ от 06.04.2011 г. №63-ФЗ «Об электронной подписи», являются простая и усиленная электронная подпись.

Public Key Infrastructure (Инфраструктура открытых ключей — PKI) — интегрированный набор служб и средств администрирования для создания и развертывания приложений, использующих криптографию с открытыми ключами; обеспечивает функции управления открытыми ключами.

Public Key Cryptography Standarts (PKCS) – стандарты криптографии с открытым ключом, разработанные компанией RSA Security. Удостоверяющий центр осуществляет свою работу в соответствии со следующими стандартами PKCS:

- ***CMS (PKCS#7)*** – стандарт, определяющий формат и синтаксис криптографических сообщений в соответствии с RFC 3852.
- ***PKCS#10*** – стандарт, определяющий формат и синтаксис запроса на сертификат ЭП в соответствии с RFC 2986.
- ***CMC*** – стандарт, определяющий формат и синтаксис запроса на сертификат ЭП в соответствии с RFC 5272.

Прочие термины имеют то же определение, что и в Федеральном законе РФ от 06.04.2011 г. №63-ФЗ «Об электронной подписи».

1.2. Сведения об Удостоверяющем центре «e-Notary»

Удостоверяющий центр, именуемый «e-Notary» (далее – УЦ «e-Notary» или УЦ), является структурным подразделением акционерного общества (АО) «СИГНАЛ-КОМ».

АО «СИГНАЛ-КОМ» реализует целевые функции аккредитованного удостоверяющего центра по изготовлению и обслуживанию квалифицированных сертификатов ключей проверки электронной подписи в соответствии с Федеральным законом Российской Федерации от 06.04.2011 г. №63-ФЗ «Об электронной подписи» (далее — №63-ФЗ «Об ЭП») и осуществляет свою деятельность на территории Российской Федерации в соответствии с Уставом и на основании следующих документов:

- Свидетельство о государственной аккредитации удостоверяющего центра, выданное Министерством связи и массовых коммуникаций Российской Федерации от 10.07.2017 г., Регистрационный № 730;
- Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России ЛСЗ №0016606, рег. № 17527 Н от 06.11.2019 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области

шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

РЕКВИЗИТЫ АО «СИГНАЛ-КОМ»:

Полное наименование: Акционерное общество «СИГНАЛ-КОМ»

Юридический адрес: 115088, г. Москва, набережная Крутицкая, дом 23, квартира 64.

Адрес местонахождения Удостоверяющего центра: 115088, Москва, Угрешская ул., дом 2, строение 15.

Почтовый адрес: 115193, Москва, а/я №6.

Банковские реквизиты:

- Р/с: 40702810800000000193 в АО «Банк Русский Стандарт», г. Москва
- БИК: 044525151
- К/с: 30101810845250000151 в ГУ Банка России по ЦФО

ИНН/КПП: 7714028893/772501001

ОГРН: 1027700239863

Контактные телефоны: +7 (495) 663-3073, 663-3034, 663-3093.

Адрес электронной почты: signal@signal-com.ru, signal@gin.ru, e-notary@signal-com.ru.

Часы работы офиса: понедельник — пятница, с 09:00 до 18:00.

Часы приема клиентов: понедельник — пятница, с 10:00 до 17:10.

Часы работы ПАК УЦ: круглосуточно.

Порядок информирования о предоставлении услуг удостоверяющего центра:

Информация о предоставлении услуг Удостоверяющего центра размещена на сайте Удостоверяющего центра https://www.e-notary.ru.

Адреса местонахождения, телефоны, адреса электронной почты опубликованы на официальном сайте УЦ по адресу https://www.e-notary.ru/info/contacts.

Информация о времени посещения офиса УЦ можно получить, обратившись в Удостоверяющий центр по телефону или электронной почте, указанным на официальном сайте УЦ по адресу – https://www.e-notary.ru/info/contacts.

1.3. Общие сведения о Регламенте

1.3.1. Статус регламента

Настоящий Регламент в соответствии с Приказом Минцифры России от 13.11.2020г. № 584 является порядком реализации функций аккредитованного удостоверяющего центра УЦ «e-Notary» и исполнения его обязанностей. Регламент содержит общий набор правил, определяющих условия предоставления услуг УЦ «e-Notary», включая права, обязанности и ответственность Удостоверяющего центра и Пользователей УЦ, присоединившихся к Регламенту в порядке, предусмотренном статьей 428 Гражданского кодекса Российской Федерации.

Настоящий Регламент является Соглашением, налагающим обязательства на все вовлеченные Стороны, а также служит средством официального уведомления и информирования всех Сторон о взаимоотношениях, возникающих в процессе предоставления и использования услуг УЦ.

Регламент разработан в соответствии с законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, а его структура и содержание соответствуют требованиям Приказа Министерства цифрового развития, связи и массовых коммуникаций РФ от 13 ноября 2020 г. № 584 "Об утверждении Требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей" и рекомендации RFC 3647 («Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework»).

1.3.2. Идентификация Регламента

Полное наименование настоящего документа – «Удостоверяющий центр e-Notary. Регламент».

Текущий номер версии документа – 02/2021.

Дата создания документа – 02 февраля 2021 года.

Объектный идентификатор (OID), присвоенный документу — 1.3.6.1.4.1.5849.3.2.

1.3.3. Присоединение к Регламенту

Присоединение к настоящему Регламенту осуществляется путем подписания и предоставления заинтересованным лицом в Удостоверяющий центр заявления о присоединении к Регламенту по форме Приложения 1 настоящего Регламента.

С момента регистрации заявления о присоединении к Регламенту в Удостоверяющем центре лицо, подавшее заявление, считается присоединившимся к Регламенту и является Стороной Регламента.

Факт присоединения лица к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент регистрации заявления о присоединении в реестре Удостоверяющего центра. Лицо, присоединившееся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

После присоединения к Регламенту Удостоверяющий центр и Сторона, присоединившаяся к Регламенту, вступают в соответствующие договорные отношения на неопределённый срок.

1.3.4. Публикации Регламента и его изменений

Настоящий Регламент и уведомления о его изменениях распространяются в электронном виде путем публикации на Портале УЦ e-Notary по адресу: https://www.e-notary.ru/info/reglament/.

Изменения и дополнения в Регламент, включая приложения к нему, вносятся Удостоверяющим центром в одностороннем порядке.

УЦ вправе самостоятельно определять сроки и порядок вступления в силу изменений и дополнений в Регламент УЦ.

Все изменения, вносимые Удостоверяющим центром в Регламент по собственной инициативе, вступают в силу по истечению 10 (десяти) дней с момента размещения его новой редакции по адресу https://www.e-notary.ru/info/reglament/, если иной срок не указан при таком размещении.

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

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 в силу. Сторона, несогласная с изменениями Регламента, имеет право до вступления в силу таких изменений на расторжение Регламента в порядке, предусмотренном п. 1.3.7 настоящего Регламента.

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

1.3.5. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его публикации и действует до прекращения деятельности УЦ.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в п. 1.3.4 о публикации Регламента.

В случае прекращения действия Регламента Удостоверяющий центр уведомляет об этом за 30 (тридцать) календарных дней до даты прекращения его действия.

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

1.3.6. Разрешение споров

Сторонами в споре, в случае его возникновения, считаются Удостоверяющий центр и Пользователь УЦ, присоединившийся к Регламенту.

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

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

Спорные вопросы между Сторонами, не урегулированные в процессе переговоров, решаются в Арбитражном суде города Москвы в соответствии с действующим законодательством Российской Федерации.

1.3.7. Порядок расторжения Регламента

Действие настоящего Регламента может быть прекращено по инициативе одной из Сторон в следующих случаях:

- по собственному желанию одной из Сторон;
- при нарушении одной из Сторон условий настоящего Регламента.

В случае расторжения Регламента инициативная Сторона письменно уведомляет другую Сторону о своих намерениях за 30 (тридцать) календарных дней до даты расторжения Регламента. Регламент считается расторгнутым после выполнения Сторонами своих обязательств и проведения взаиморасчетов согласно условиям Регламента.

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

1.3.8. Применение регламента

Нормы, содержащиеся в Регламенте, становятся обязательными для Пользователя УЦ с момента предоставления заинтересованным лицом в Удостоверяющий центр заявления о присоединении к Регламенту.

С момента регистрации заявления лицо, подавшее заявление, считается присоединившимся к Регламенту и является Стороной Регламента.

Стороны согласны с тем, что условия настоящего Регламента принимаются Пользователем полностью без каких либо изъятий, изменений и протоколов разногласий.

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.

В случае противоречия и/или расхождения положений какого-либо приложения к настоящему Регламенту с положениями собственно Регламента, Стороны считают доминирующим смысл и формулировки Регламента.

1.4. Оплата услуг Удостоверяющего центра. Сроки и порядок расчетов

Услуги формирования ключей ЭП, изготовления и обслуживания сертификатов, выдачи съемных ключевых носителей и средств электронной подписи (криптографические приложения для генерации ключей и запросов сертификатов, построенные на базе СКЗИ, сертифицированных ФСБ России), а также услуги проверки электронных подписей в электронных документах предоставляются Удостоверяющим центром на платной основе.

Стоимость и состав услуг УЦ определяются текущими тарифами Удостоверяющего центра, которые публикуются на страницах сайта http://www.e-notary.ru.

Сформировать Заявку для получения счета на оплату товаров и оказание услуг УЦ можно одним из следующих способов:

- обратиться в УЦ e-Notary по телефонам +7 (495) 663-3073, (495) 663-3093, (495)663-3034 или по адресу e-notary@signal-com.ru;

- оформить Заявку на странице Портала e-Notary https://www.e-notary.ru/packages/ и получить счет на оплату услуг УЦ на адрес электронной почты, указанный в Заявке.

Если формирование ключей и запроса на сертификат Пользователь УЦ будет выполнять самостоятельно, он должен включить в Заявку программное обеспечение (ПО), необходимое для генерации ключей и запросов на сертификаты с использованием российских криптографических стандартов, если такое ПО Пользователем УЦ ранее не приобреталось или не было получено иным образом. Выбор конкретного ПО для генерации ключей и запросов на сертификат зависит от средства электронной подписи, которое Пользователь УЦ в дальнейшем будет использовать в своей работе.

На основании Заявки Удостоверяющий центр выставляет Стороне, присоединившейся к Регламенту, счет на оплату изготовления сертификата ключа проверки ЭП и, если это необходимо, на ключевые носители и программное обеспечение для генерации ключей и запроса на сертификат.

Сроки и порядок расчетов за услуги, оказываемые УЦ, регулируются условиями Договора публичной оферты (https://www.e-notary.ru/info/contracts_offer) между УЦ и Стороной, присоединившейся к Регламенту.

Оплата услуг может осуществляться как путем полной предоплаты (аванса), так и путем частичной предоплаты или в случае заключения контрактов по итогам проведения закупочных процедур, то есть по факту оказания услуг.

После поступления денежных средств на расчетный счет УЦ, клиент получает на адрес электронной почты, указанный в Заявке, информационное письмо с подтверждением поступления денежных средств, информацией о комплекте необходимых для получения услуг документов и порядке предоставлении услуг. Далее клиенту необходимо обратиться в Удостоверяющий центр по телефону или электронной почте, указанным на официальном сайте УЦ по адресу https://www.e-notary.ru/info/contacts, и согласовать дату посещения офиса Центра Регистрации.

Если иное не предусмотрено Договором, изготовление сертификата ключа проверки ЭП осуществляется после оплаты услуг УЦ путем полной/частичной предоплаты, но не позднее 5 (пяти) рабочих дней, следующих за рабочим днем, и только после предоставления комплекта документов, необходимых для изготовления сертификата.

Срок и порядок расчетов могут быть пересмотрены по согласованию с Заявителем, в том числе отдельно заключаемыми соглашениями между Заявителем и Удостоверяющим центром.

При оказании услуг по итогам проведения закупочных процедур порядок и срок оказания услуг устанавливаются в соответствии с положениями заключенных контрактов.

В случае внеплановой смены ключей ЭП Удостоверяющего центра, Удостоверяющий центр выполняет обновление сертификатов Пользователей УЦ безвозмездно.

УЦ обеспечивает безвозмездный доступ к СОС и к Справочнику сертификатов, доступным через Web-интерфейс на Портале УЦ e-Notary (https://www.e-notary.ru/services).

УЦ безвозмездно выдает копии сертификатов в форме документов на бумажном носителе, выполняет действия по аннулированию сертификатов, осуществляет по обращению лица, которому выдан сертификат, регистрацию указанного лица в Единой системе идентификации и аутентификации, предоставляет Руководство по обеспечению безопасности

использования электронной подписи и средств электронной подписи, а также иных инструкций по работе со средствами криптографической защиты информации и информационной безопасности.

1.5. Финансовая ответственность

Удостоверяющий центр не несет никакой ответственности в случае нарушения Пользователями УЦ положений настоящего Регламента.

Удостоверяющий центр не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если Удостоверяющий центр обоснованно полагался на сведения, указанные в заявлениях и предоставленных документах Пользователя УЦ, присоединившегося к Регламенту.

Удостоверяющий центр несет ответственность за убытки при использовании ключа ЭП и сертификата ключа проверки ЭП Пользователя УЦ только в случае, если данные убытки возникли вследствие компрометации ключа ЭП Удостоверяющего центра, или вследствие несоответствия сведений в сертификате сведениям, указанным в заявлении на изготовление сертификата.

Финансовая ответственность за убытки, причиненные третьим лицам аккредитованным УЦ, определяется положением ст.16, п.3, подпункт 2 Федерального закона №63-ФЗ «Об ЭП».

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

1.6. Прекращение деятельности Удостоверяющего центра

Деятельность Удостоверяющего центра может быть прекращена в порядке, установленном законодательством Российской Федерации.

В случае прекращения деятельности Удостоверяющего центра, Владельцы сертификатов, срок действия которых еще не истек, должны быть извещены об этом в письменной форме за 1 (один) месяц до даты прекращения деятельности УЦ.

В случае прекращения деятельности Удостоверяющего центра, выданные им сертификаты ключей проверки ЭП передаются на обслуживание другому Удостоверяющему центру. Сертификаты ключей проверки ЭП, не переданные в другой Удостоверяющий центр, аннулируются (отзываются) или передаются на хранение в соответствии с положениями ч.6, ст.13 №63-ФЗ «Об ЭП».

Прекращение деятельности аккредитованного УЦ регулируется положениями ст.15. п.4 Федерального закона №63-ФЗ «Об ЭП».

1.7. Контактная информация

По всем вопросам, касающимся положений настоящего Регламента, следует обращаться к уполномоченному представителю УЦ, отвечающему за регистрацию, обслуживание и интерпретацию Регламента:

Полное наименование юридического лица: АО «СИГНАЛ-КОМ»

Почтовый адрес: 115193, Москва, а/я №6

Адрес электронной почты: admin@e-notary.ru , signal@signal-com.ru

Телефон: +7 (495) 663-3073, 663-3034, 663-3093

Контактное лицо: Зам.руководителя УЦ e-Notary Карпов Илья Олегович

2. Положения об удостоверяющем центре

2.1. Инфраструктура УЦ e-Notary

Выполнение всех услуг по управлению ключами электронной подписи (далее – ключи ЭП) и сертификатами ключей проверки электронной подписи (далее — сертификаты ключей проверки ЭП, сертификаты) в УЦ e-Notary осуществляется с использованием программно-аппаратного комплекса (ПАК) УЦ «Notary-PRO 2.8» (Заключение ФСБ России № 149/7/6/114 от 27.03.2020 - ранее с использованием программно-аппаратного комплекса УЦ «Notary-PRO» версии 2.7 (сертификат соответствия ФСБ России №СФ/128-3205 от 06.11.2017 г.)), СКЗИ «Крипто-КОМ 3.3» (сертификаты соответствия ФСБ России №№ СФ/114-3615, СФ/124-3616 от 29.12.2018 г. для исполнений 7 и 8, соответственно), СКЗИ «Крипто-КОМ 3.4» (сертификаты соответствия ФСБ России №№ СФ/114-3975, СФ/124-3976 от 11.01.2021 г. для исполнений 42 и 43, соответственно), СКЗИ «CADB 2.1» (сертификаты соответствия ФСБ России №№ СФ/114-3755, СФ/124-3756 от 18.09.2019 г. для исполнений 1 и 2, соответственно) и СКЗИ «Signal-COM JCP 3.1» (сертификаты соответствия ФСБ России №№ СФ/114-3753, СФ/124-3754 от 18.09.2019 г. для исполнений 1 и 2, соответственно) разработки АО «СИГНАЛ-КОМ».

ПАК УЦ «Notary-PRO 2.8» (далее — ПАК УЦ соответствует требованиям ФСБ России к средствам удостоверяющего центра, утвержденным приказом ФСБ России от 27.12.2011г. № 796, и требованиям к информационной безопасности удостоверяющих центров, установленным для класса КС2, а также требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утвержденным приказом ФСБ России от 27.12.2011г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Наличие государственной аккредитации Министерства связи и массовых коммуникаций Российской Федерации (Свидетельство об аккредитации Рег.№ 730 от 10.07.2017 г.) дает УЦ «e-Notary» право на изготовление и обслуживание **квалифицированных** сертификатов ключей проверки ЭП (далее — квалифицированные сертификаты).

Инфраструктура ПАК УЦ включает:

- Удостоверяющий центр;
- Регистрационные центры;
- Справочник сертификатов;
- Web-интерфейс Удостоверяющего центра.

2.1.1. Удостоверяющий центр. Перечень функций и услуг

Удостоверяющий центр на базе ПАК УЦ обеспечивает выполнение интегрированного набора услуг сертификационного центра и регистрационного центра, и в процессе своей деятельности реализует следующие функции:

1. первичная идентификация и аутентификация лиц, обратившихся в УЦ за получением сертификатов (Заявители): установление личности получателя сертификата (Заявителя) либо полномочия лица, выступающего от имени заявителя по обращению за получением сертификата;

2. регистрация Заявителей в реестре УЦ;
3. предоставление Заявителю средств ЭП для самостоятельного формирования ключей ЭП, ключей проверки ЭП и запроса на сертификат или формирование ключей и запросов на сертификаты по обращению Заявителей силами штатных сотрудников УЦ с гарантией обеспечения конфиденциальности ключа ЭП;
4. прием и регистрацию от Заявителей запросов на сертификаты;
5. подтверждение владения Заявителем ключом ЭП, соответствующим ключу проверки ЭП, указанному в запросе на сертификат;
6. контроль уникальности ключей проверки ЭП в регистрируемых запросах;
7. установление сроков действия сертификатов;
8. изготовление на основании запросов электронных сертификатов ключей проверки ЭП и передача их Заявителям;
9. в случае формирования ключей по обращению Заявителя — передача Заявителю ключевого носителя, содержащего его ключ ЭП, сформированный сертификат и другие необходимые данные;
10. изготовление копий сертификатов в форме документов на бумажных носителях;
11. передача Заявителям бумажных копий сертификатов, полученных из УЦ, и ознакомление их под расписку с информацией, содержащейся в сертификате (обязательно для квалифицированных сертификатов, см. ч.3 ст.18 №63-ФЗ «Об ЭП»);
12. предоставляет руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (см. Приложение № 8);
13. аутентификация Владельцев сертификатов, запрашивающих аннулирование (отзыв сертификатов;
14. аннулирование сертификата по требованию Владельца сертификата, либо по решению административных служб УЦ, в том числе в соответствии с ч.6.1 ст.14 №63-ФЗ «Об ЭП»; аннулирование сертификата для юридических лиц может быть также проведено на основании письменного заявления полномочного представителя юридического лица;
15. выпуск СОС;
16. ведение реестра выпущенных сертификатов и СОС;
17. публикация выпущенных сертификатов и СОС в общедоступном сетевом Справочнике сертификатов;
18. подтверждение подлинности электронных подписей в документах, представленных в электронной форме, по обращениям Пользователей УЦ;
19. формирование ключей ЭП и ключей проверки ЭП Удостоверяющего центра;
20. формирование запросов с ключами проверки ЭП Удостоверяющего центра для получения квалифицированного сертификата аккредитованного УЦ в вышестоящем головном УЦ;
21. осуществление иных функций, связанных с использованием ЭП, установленных законодательством Российской Федерации.

2.1.2. Регистрационные центры. Перечень функций и услуг

Регистрационный центр (РЦ) – субъект инфраструктуры PKI, которые регистрируют лиц, обратившихся в УЦ за получением сертификатов (Заявителей), их первичной идентификации и аутентификации. РЦ регистрирует запросы на выпуск и отзыв сертификатов ключей проверки ЭП, обеспечивает их доставку в УЦ и отвечает за передачу сформированных сертификатов и их бумажных копий Заявителям.

В процессе своей деятельности Регистрационный центр реализует следующие функции:

1. первичная идентификация и аутентификация Заявителей (установление личности получателя сертификата либо полномочия лица, выступающего от его имени по обращению за получением сертификата);

2. регистрация Заявителей в реестре УЦ;
3. предоставление Заявителю средств ЭП для самостоятельного формирования ключей ЭП, ключей проверки ЭП и запроса на сертификат или формирование ключей и запросов на сертификаты по обращению Заявителей силами штатных сотрудников УЦ с гарантией обеспечения конфиденциальности ключа ЭП;
4. прием запросов на сертификаты от Заявителей;
5. установление сроков действия сертификатов;
6. передача в УЦ запросов на сертификаты и санкционирование изготовления сертификатов по запросам Заявителей;
7. передача Заявителям изготовленных сертификатов в электронной форме;
8. в случае формирования ключей по обращению Заявителя — передача Заявителю ключевого носителя, содержащего его ключ ЭП, сформированный сертификат и другие необходимые данные;
9. изготовление копий сертификатов в форме документов на бумажных носителях;
10. передача Заявителям бумажных копий сертификатов, полученных из УЦ, и ознакомление их под расписку с информацией, содержащейся в сертификате (обязательно для квалифицированных сертификатов, см. ч.3, ст. 18 №63-ФЗ «Об ЭП»);
11. предоставление руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;
12. аутентификация Владельцев сертификатов, запрашивающих аннулирование (отзыв) сертификатов;
13. прием от Владельцев сертификатов запросов на аннулирование (отзыв) сертификата и передача их в УЦ; аннулирование сертификата для юридических лиц может быть выполнено на основании письменного заявления полномочного представителя юридического лица.

Регистрационные центры построены на базе сертифицированного ФСБ России ПО «Notary-PRO RA» из состава ПАК УЦ и обладают необходимым комплексом криптографических средств, обеспечивающих защищенное взаимодействие РЦ с ПАК УЦ в режиме on-line.

В УЦ e-Notary выполнение указанных выше функций возлагается на центральный Регистрационный центр АО «СИГНАЛ-КОМ» в лице его сотрудников, которые назначаются ответственными за регистрацию и обслуживание Заявителей.

2.1.3. Справочник сертификатов

Справочник сертификатов — субъект инфраструктуры PKI, обеспечивающий хранение сертификатов ключей проверки ЭП и Списков отозванных сертификатов (СОС), формируемых в УЦ.

В инфраструктуре УЦ e-Notary выданные сертификаты публикуются в специализированный сетевой Справочник сертификатов на базе сервера LDAP. Внесение изменений в Справочник сертификатов с целью публикации новых сертификатов и СОС выполняется в УЦ автоматически, при их формировании.

Справочник сертификатов УЦ e-Notary обеспечивает реализацию следующих целевых функций:

- прием и регистрацию сертификатов ключей проверки ЭП и СОС, поступающих из УЦ;
- свободный доступ к справочнику сертификатов и СОС;
- поддержку поисковой системы сертификатов ключей проверки ЭП и СОС;
- Web-интерфейс к интерактивной поисковой системе сертификатов ключей проверки ЭП и СОС.

Справочник сертификатов УЦ e-Notary доступен через Web-интерфейс Портала УЦ e-Notary по адресу: https://www.e-notary.ru/services.

2.1.4. Web-интерфейс УЦ

Web-интерфейс УЦ e-Notary обеспечивает защищенное взаимодействие удаленных Заявителей с Удостоверяющим центром в процессе генерации ключей и запросов на сертификаты (PKCS#10 и CMC) на страницах Web-интерфейса, с последующей передачей сформированных запросов в УЦ и доставкой изготовленных сертификатов на рабочие места Заявителей. Взаимодействие обеспечивается с использованием протокола https и стандартных средств браузеров Internet Explorer, Google Chrome, Mozilla FireFox, Opera, Яндекс.Браузер.

Запросы на сертификаты, переданные в УЦ e-Notary через Web-интерфейс УЦ, могут быть сертифицированы только после доставки и проверки в УЦ комплекта документов, удостоверяющих личность Заявителя, идентификации личности и подтверждения достоверности данных, поступивших в запросе на сертификат.

2.2. Пользователи УЦ

Пользователями услуг УЦ являются участники прикладных защищенных информационных систем и систем электронного документооборота, подразделяемые на Владельцев сертификатов и Пользователей сертификатов, выпускаемых данным УЦ.

Владельцы сертификатов ключей проверки ЭП – зарегистрированные в УЦ лица, получившие сертификаты ключей проверки ЭП в результате успешного выполнения специальной регистрационной процедуры. Владельцами сертификата могут быть признаны:

- отдельные самостоятельные физические лица (включая индивидуальных предпринимателей);
- юридическое лицо и физическое лицо, действующее от имени юридического лица по доверенности или на основании уставных документов, дающих право данному физическому лицу представлять юридическое лицо и пользоваться услугами Удостоверяющего центра;
- юридическое лицо (без указания физического лица, действующего от имени юридического лица), в случае изготовления сертификата, используемого для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе при оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также в иных случаях, предусмотренных федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами.

Пользователи сертификатов ключей проверки ЭП – любое лицо, устройство или программное приложение, которые могут не иметь собственных сертификатов, но используют полученные в УЦ сведения о сертификате для проверки принадлежности электронной подписи в электронном документе Владельцу сертификата и (или) для зашифрования адресованной ему информации.

Пользователи сертификатов сами могут быть Владельцами сертификатов.

Пользователи и Владельцы сертификатов являются Пользователями УЦ.

2.3. Разновидности сертификатов и области их применения

2.3.1. Виды сертификатов

В рамках УЦ «e-Notary» обеспечивается изготовление и обслуживание усиленных квалифицированных сертификатов ключей проверки электронной подписи.

В соответствии с требованиями пункта 2.1 статьи 15 №63-ФЗ «Об ЭП», для подписания квалифицированных сертификатов Пользователей используются квалифицированные сертификаты аккредитованного УЦ, выданные головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган.

Аккредитованному УЦ запрещается использовать квалифицированные сертификаты, выданные головным удостоверяющим центром, для подписания сертификатов, не являющихся квалифицированными.

Квалифицированные сертификаты аккредитованного УЦ, выданные головным удостоверяющим центром, внесены в реестр сертификатов аккредитованных удостоверяющих центров (https://e-trust.gosuslugi.ru/CA) на портале уполномоченного федерального органа в области использования электронной подписи, и опубликованы в Справочнике квалифицированных сертификатов, доступном через портал УЦ e-Notary на странице https://search-qua.e-notary.ru/.

Перечень услуг, предоставляемый УЦ e-Notary Владельцам и Пользователям квалифицированных сертификатов, перечислен в пп. 2.1.1, 2.1.2 настоящего Регламента.

2.3.2. Сведения и документы, необходимые для изготовления сертификатов

Квалифицированные сертификаты ключа проверки ЭП выдаются только при наличии документов или их надлежащим образом заверенных копий, необходимых для удостоверения личности Заявителя, а также при наличии сведений, на основании которых УЦ запрашивает из государственных информационных ресурсов данные, необходимые для подтверждения информации, включаемой в состав сертификата.

Перечень документов и сведений, запрашиваемых Удостоверяющим центром у Заявителя для изготовления и выдачи сертификата, приводится в п. 3.1.1.3 настоящего Регламента.

2.3.3. Разрешенные области применения сертификатов

Квалифицированные сертификаты могут использоваться для защиты электронных документов (формирование/проверка ЭП, шифрование/расшифрование) в любых системах юридически значимого электронного документооборота, а также для аутентификации взаимодействующих сторон и защиты трафика между ними в защищенных клиент-серверных приложениях и распределенных системах передачи данных.

2.4. Права Удостоверяющего центра и Пользователя УЦ

2.4.1. Права УЦ e-Notary

В рамках предоставления услуг и выполнения функций, предусмотренных статьями 13 и 15 №63-ФЗ «Об ЭП», Удостоверяющий центр имеет право:

- запрашивать у Заявителя документы для подтверждения любой информации, содержащейся в заявлении на изготовление и выдачу сертификата ключа проверки ЭП;
- с использованием инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, запрашивать и получать у операторов государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных Заявителем;
- запрашивать и получать из государственных информационных ресурсов:

    - выписку из единого государственного реестра юридических лиц в отношении заявителя-юридического лица;
    - выписку из единого государственного реестра индивидуальных предпринимателей в отношении заявителя — индивидуального предпринимателя;
    - выписку из единого государственного реестра налогоплательщиков в отношении заявителя – иностранной организации;
- запрашивать у Заявителя дополнительные документы, подтверждающие достоверность представленных им сведений, в случае наличия противоречий между сведениями, представленными Заявителем и сведениями, полученными Удостоверяющим центром из государственных информационных ресурсов;
- не принимать от заявителя документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;
- отказать Заявителю в регистрации в УЦ в случае непредоставления или ненадлежащего оформления необходимых регистрационных документов, а также в случае, когда подлинность документов вызывает сомнение;
- отказать Заявителю в выдаче сертификата ключа проверки ЭП в случае невыполнения заявителем обязанностей, установленных №63-ФЗ «Об ЭП», принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом;
- отказать Заявителю в изготовлении сертификата в случае ненадлежащего оформления заявления на его изготовление;
- отказать Заявителю в изготовлении сертификата в случае, если не было подтверждено, что заявитель владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному заявителем для получения квалифицированного сертификата;
- отказать Заявителю в изготовлении сертификата в случае отрицательного результата проверки в реестре сертификатов УЦ уникальности ключа проверки ЭП, указанного Заявителем для получения сертификата;
- отказать Владельцу сертификата в аннулировании (отзыве) сертификата в случае, если сертификат уже аннулирован или истек установленный срок действия этого сертификата.
- отказать Владельцу сертификата в приостановлении/возобновлении действия сертификата в случае ненадлежащего оформления заявления на приостановление/возобновление действия сертификата или в случае, если истек срок действия этого сертификата или истек срок, на который сертификат был приостановлен;
- без заявления Владельца сертификата аннулировать (отозвать) сертификат в случае невыполнения Владельцем обязанностей, установленных законодательством Российской Федерации в области электронной подписи, настоящим Регламентом, а также в случае появления у удостоверяющего центра достоверных сведений о том, что документы, представленные Заявителем для изготовления сертификата, не являются подлинными и (или) не подтверждают достоверность всей информации, включаемой в сертификат и/или в случае, если услуга по изготовлению и выдаче сертификата не оплачена в надлежащем порядке;
- аннулировать (отозвать) сертификат Владельца в случае:
    - обращения (письменного или по телефону) Владельца сертификата ключа проверки ЭП
    - установленного факта компрометации соответствующего ключа ЭП, с уведомлением Владельца аннулированного (отозванного) сертификата и указанием обоснованных причин;
    - если УЦ стало известно о прекращении действия документа, на основании которого оформлен сертификат;
    - если установлено, что в результате технической ошибки сертификат содержит недостоверные или неполные сведения;
    - указания лиц или органов, имеющих такое право в силу закона.
- требовать от Заявителей оплаты услуг УЦ;
- в одностороннем порядке изменять тарифы, путем публикации новых тарифов на страницах сайта http://www.e-notary.ru;

- по обращению Владельцев сертификатов выступать в качестве эксперта по вопросам применения ЭП и средств ЭП в случае возникновения споров между Владельцем и иными пользователями PKI.

2.4.2. Права Пользователей УЦ

Пользователь УЦ e-Notary имеет право:

1. получить сертификат ключа проверки ЭП Удостоверяющего центра;
2. получить СОС, изготовленный в УЦ;
3. применять сертификат ключа проверки ЭП Удостоверяющего центра для проверки электронной подписи УЦ в сертификатах, изготовленных в УЦ;
4. применять СОС, изготовленный в УЦ, для проверки статуса сертификатов, изготовленных в УЦ;
5. получать в электронной форме сертификаты ключей ЭП, выпущенные в УЦ и опубликованные в сетевом Справочнике сертификатов;
6. применять сертификаты, полученные из Справочника сертификатов, для проверки электронных подписей электронных документов в соответствии со сведениями, указанными в сертификатах;
7. обратиться в УЦ за подтверждением подлинности сертификатов, выпущенных УЦ;
8. обратиться в УЦ за подтверждением подлинности электронных подписей в электронных документах;
9. обратиться в УЦ для приобретения средств электронной подписи (включая средства генерации ключей и запросов на сертификаты);
10. обратиться в УЦ с заявлением на формирование ключей ЭП, ключей проверки ЭП и изготовление сертификата с записью полученных данных на ключевой носитель.

2.4.3. Права Владельцев сертификатов

В дополнение к правам Пользователей УЦ, Владельцы сертификатов имеют право:

1. обратиться в УЦ для аннулирования (отзыва) сертификата ключа проверки ЭП, если период действия этого сертификата еще не истек;
2. консультироваться в УЦ по всем вопросам, связанным с использованием сертификатов и электронной подписи.

2.5. Обязанности Удостоверяющего центра и Пользователей УЦ

2.5.1. Обязанности Удостоверяющего центра

УЦ e-Notary должен строго соблюдать правила, изложенные в настоящем Регламенте, в частности:

в отношении ключей и сертификатов УЦ:

- использовать ключ ЭП Удостоверяющего центра только для заверения издаваемых им сертификатов и Списков отозванных сертификатов;
- использовать квалифицированный сертификат аккредитованного ПАК УЦ, выданный головным удостоверяющим центром, функции которого осуществляет уполномоченный федеральный орган, только для подписания квалифицированных сертификатов Пользователей;
- обеспечивать надежную защиту ключа ЭП Удостоверяющего центра от несанкционированного доступа;

в отношении регистрации Заявителей:

- осуществлять регистрацию Заявителей в реестре УЦ по их заявлению на регистрацию;
- осуществлять первичную идентификацию и аутентификацию Заявителей в соответствии с положениями настоящего Регламента;
- установить личность Заявителя — физического лица, обратившегося в УЦ за получением сертификата;
- получить от лица, выступающего от имени Заявителя — юридического лица, подтверждение правомочия обращаться за получением сертификата;

в отношении изготовления ключей для Заявителей:

- по обращению зарегистрированного Заявителя обеспечивать формирование на съемный ключевой носитель его ключа ЭП и ключа проверки ЭП, а также запросов сертификатов с помощью сертифицированного средства ЭП (опциональная услуга);
- обеспечивать конфиденциальность в отношении изготовляемых ключей ЭП Заявителей;

в отношении изготовления и выдачи сертификатов:

- принимать и обрабатывать запросы на сертификацию и изготавливать сертификаты:

    - осуществлять регистрацию поступающих запросов сертификатов;
    - осуществлять изготовление сертификатов ключей проверки ЭП на основании и в соответствии с запросами на сертификаты;
    - вносить в выпускаемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;
    - обеспечивать уникальность регистрационной информации Заявителей, включаемой в атрибуты сертификата;
    - соблюдать конфиденциальность в отношении регистрационной информации о Заявителе;
    - вести реестр выпущенных сертификатов;
    - обеспечивать уникальность серийных номеров изготавливаемых сертификатов;
    - обеспечивать уникальность ключей проверки ЭП в составе изготавливаемых сертификатов (отказывать Заявителю в изготовлении сертификата в случае отрицательного результата проверки в реестре сертификатов УЦ уникальности ключа проверки ЭП, указанного Заявителем запросе на получение сертификата);
    - отказывать Заявителю в изготовлении сертификата в случае, если не было подтверждено, что Заявитель владеет ключом ЭП, который соответствует ключу проверки ЭП, указанному Заявителем в запросе на получение сертификата;
    - изготавливать копии сертификатов на бумажном носителе;
    - уведомлять Заявителя о выпуске запрошенного им сертификата;
    - передавать сформированные сертификаты и их бумажные копии Заявителям или уполномоченным представителям УЦ для передачи Заявителям;
    - обеспечить архивное хранение сертификатов в электронном виде в течение всего срока действия сертификатов;

- публиковать выпущенные квалифицированные сертификаты в сетевом Справочнике сертификатов, доступном всем Пользователям УЦ;
- направлять в Единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра);

- по заявлению Владельца квалифицированного сертификата безвозмездно осуществлять регистрацию указанного лица в единой системе идентификации и аутентификации (ЕАИС);

в отношении аннулирования (отзыва) сертификатов:

- принимать и обрабатывать запросы от Владельцев сертификатов на аннулирование (отзыв) действия сертификатов:

    - принимать и обрабатывать запросы на аннулирование (отзыв) сертификатов;
    - аутентифицировать Заявителя, запрашивающего аннулирование (отзыв) сертификата;
    - аннулировать (отзывать) сертификаты по запросам Владельцев и РЦ;
    - информировать Владельцев и Пользователей Сертификатов об аннулирование (отзыве) действия сертификатов путем ежедневного (по расписанию) и внепланового (по факту отзыва, см. п.3.5) выпуска СОС и публикации их в точках распространения СОС, указанных в расширении CDP (CRLDistributionPoint) сертификатов;

- уведомлять Владельца сертификата о фактах, которые стали известны УЦ и которые существенным образом могут сказаться на возможности дальнейшего использования сертификатов его ключей;

в отношении Справочника сертификатов:

- обеспечивать своевременную публикацию сертификатов и СОС в общедоступном сетевом Справочнике сертификатов;
- обеспечивать защиту Справочника сертификатов от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;
- обеспечить любому лицу безвозмездный доступ с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", к Справочника сертификатов в любое время в течение срока деятельности Удостоверяющего центра, если иное не установлено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами;

в отношении синхронизации времени:

- обеспечивать работу служб УЦ по GMT (Greenwich Mean Time) с учетом часового пояса;
- обеспечивать синхронизацию по времени всех программных и технических средств УЦ в соответствии с их предназначением;

в отношении оказания дополнительных услуг:

- информировать заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, а также о мерах, необходимых для обеспечения безопасности ключей электронных подписей;
- на платной основе предоставлять Владельцам и Пользователям сертификатов программное обеспечение и ключевую информацию, необходимую для работы в защищенной прикладной системе;
- по запросам Владельцев сертификатов и Пользователей УЦ обеспечивать подтверждение подлинности электронных подписей в документах, представленных в электронной форме;
- консультировать Владельцев по всем вопросам, связанным с использованием сертификата; консультирование осуществляется в порядке обмена Сторонами электронными сообщениями (e-mail: signal@signal-com.ru).

2.5.2. Обязанности заявителей

Пользователи УЦ, подающие заявления на изготовление и выдачу сертификата ключа проверки ЭП (Заявители), обязаны:

- ознакомится с положениями настоящего Регламента и Договора публичной оферты;
- оплачивать услуги УЦ в соответствии с тарифами на оказание услуг УЦ;
- точно соблюдать формат и структуру запроса сертификата, предоставляемого в УЦ, в соответствии с положениями настоящего Регламента;
- предоставлять в УЦ достоверную идентифицирующую и аутентифицирующую информацию в объеме, определенном положениями настоящего Регламента;
- указывать в запросе сертификата только достоверные сведения;
- подтверждать по требованию УЦ достоверность информации, содержащейся в сертификате ключа проверки ЭП, выдаваемом Заявителю;
- для формирования ключей ЭП и ключей проверки ЭП использовать средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с №63-ФЗ «Об ЭП».

2.5.3. Обязанности владельцев сертификатов

Владельцы сертификатов должны строго соблюдать правила, изложенные в настоящем Регламенте, в частности:

- обеспечивать сохранность ключа ЭП и ключевого носителя, принимать все возможные меры для предотвращения их потери, раскрытия, модифицирования или несанкционированного использования;
- в случае принятия решения о компрометации ключа ЭП сообщить в УЦ о факте компрометации и немедленно прекратить использование ключа ЭП;
- своевременно уведомлять УЦ о факте компрометации или подозрении на компрометацию ключа ЭП или ключевого носителя, путем подачи заявления на аннулирование (отзыв) сертификата ключа проверки ЭП;
- не использовать для формирования электронной подписи скомпрометированные ключи ЭП;
- не использовать ключи ЭП и соответствующие им сертификаты по истечении срока их действия;
- использовать ключ ЭП только для тех областей использования и с учетом тех ограничений (если таковые установлены), которые определены соответствующими полями расширения в сертификате ключа проверки ЭП (Extended Key Usage, Application Policy);
- своевременно (до истечения периода действия сертификата) осуществлять смену ключа ЭП и сертификата;
- своевременно информировать УЦ о фактах изменения данных, содержащихся в сертификатах;
- для формирования и проверки квалифицированных электронных подписей использовать средства ЭП, имеющие подтверждение соответствия требованиям, установленным в соответствии с №63-ФЗ «Об ЭП»;
- соблюдать положения настоящего Регламента.

2.6. Ответственность Удостоверяющего центра и Пользователей УЦ

2.6.1. Ответственность Удостоверяющего центра

УЦ e-Notary несет ответственность:

- за обеспечение конфиденциальности ключей ЭП Удостоверяющего центра;
- за обеспечение конфиденциальности ключей ЭП выпускаемых сертификатов (в случае формирования ключей ЭП средствами УЦ по обращению Заявителей);

- за соответствие данных в запросе сертификата и в подтверждающих документах, представленных Заявителем при регистрации в УЦ;
- за соответствие данных в сертификате сведениям, указанным в заявлении на изготовление сертификата;
- за соблюдение порядка и сроков формирования сертификатов и СОС;
- за соблюдение сроков отзыва выпущенных сертификатов.

УЦ не несет ответственности за любые прямые или косвенные убытки, любую потерю прибыли, явившиеся результатом:

- несоблюдения Владельцами сертификатов конфиденциальности собственных ключей ЭП;
- предоставления в УЦ недостоверной информации, на основании которой был изготовлен сертификат;
- несвоевременного уведомления о компрометации ключа ЭП Владельца сертификата;
- нарушения Владельцами сертификатов положений настоящего Регламента.

2.6.2. Ответственность Владельцев сертификатов

Владельцы сертификатов несут ответственность:

- за достоверность предоставляемых в УЦ сведений, на основании которых изготавливаются сертификаты;
- за последствия, возникшие в результате неисполнения им положений настоящего Регламента.

2.7. Политика конфиденциальности

Конфиденциальной считается любая информация о Владельцах сертификатов, не включенная в состав сертификатов, формируемых УЦ:

- ключ ЭП, соответствующий ключу проверки ЭП Владельца сертификата;
- аварийный пароль (ключевая фраза) для связи с УЦ по телефону;
- реестры Удостоверяющего центра, за исключением общедоступного Справочника сертификатов ключей проверки ЭП;
- отчет о проведении процедуры проверки подлинности электронной подписи в электронном документе;
- персональные данные Владельцев сертификатов, не подлежащие включению в качестве части в сертификат ключа проверки ЭП;
- информация, конфиденциальность которой охраняется Удостоверяющим центром в соответствии с договорами и локальными нормативными актами Удостоверяющего центра.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией:

- информация о настоящем Регламенте;
- сведения, включаемые в сертификаты ключей проверки ЭП и Списки отозванных сертификатов, издаваемые Удостоверяющим центром;
- актуальный Список отозванных (аннулированных) сертификатов и актуальный Справочник сертификатов.

Открытая информация может публиковаться по решению администрации Удостоверяющего центра. Место, способ и время публикации открытой информации определяется Удостоверяющим центром.

Передача конфиденциальной информации третьим лицам и уполномоченным органам государственной власти осуществляется в соответствии с действующим законодательством Российской Федерации.

2.8. Идентификация и аутентификация

2.8.1. Система именования. Уникальность имен

Имена, используемые для идентификации и аутентификации участников системы PKI и включаемые в состав сертификатов ключей проверки ЭП (совокупность атрибутов поля Subject в сертификате), должны соответствовать требованиям Федерального закона №63-ФЗ «Об ЭП», RFC 5280, а также требованиям, утвержденным приказом ФСБ России от 27.12.2011г. № 795 (для квалифицированных сертификатов). Детальные требования к составу и содержанию атрибутов имен приводится в п.2.8.2.1.

Уникальность имен, присваиваемых участникам обслуживаемых систем PKI и используемых в составе формируемых сертификатов, обеспечивается средствами Удостоверяющего центра, поэтому каждый Пользователь УЦ должен доверять ему в том, что тот не повторит дважды одного и того же имени.

2.8.2. Первичная идентификация и аутентификация Пользователя УЦ

2.8.2.1. Идентификация Пользователя УЦ

Идентификация Пользователя УЦ выполняется в процессе его регистрации в УЦ e-Notary. Результатом идентификации является присвоение Пользователю УЦ уникального имени и занесение данного имени в реестр зарегистрированных Пользователей УЦ.

Идентификация опирается на наличие у каждого Владельца сертификата уникального имени, отличного от имен всех остальных пользователей.

Уникальные имена Владельцев формируются на основании идентификационных данных, указанных в заявлении на регистрацию в УЦ и изготовление сертификата ключа проверки ЭП по форме Приложения 3, Приложения 4 настоящего Регламента. Зарегистрированные в УЦ уникальные имена Владельцев включаются в их сертификаты.

Для сертификатов приняты следующие правила назначения атрибутов уникальных имен Владельцев, включаемых в состав сертификата (символом «*» помечены поля, обязательные для заполнения при изготовлении квалифицированного сертификата):

- поля «Область/Район», «Город», «Организация», «Подразделение», «Общее имя», «Фамилия», «Отчество» заполняются на русском языке;
- поле «Страна»* заполняется двухбайтовым кодом страны (Для России — RU);
- поля «Область/Район»*, «Город»* указывают местонахождение Владельца сертификата; обязательны для юридического лица и индивидуального предпринимателя;
- поле «Адрес» содержит адрес места регистрации — юридического лица в сертификате для юридического лица и физического лица в сертификате для физического лица и индивидуального предпринимателя (название улицы и номер дома указываются по желанию Владельца сертификата);
- поле «Организация»* содержит полное или сокращенное наименование юридического лица;
- поле «Подразделение» содержит наименование подразделения, в котором работает уполномоченный представитель юридического лица;

- поле «Должность»* указывает должность физического лица, действующего от имени юридического лица на основании учредительных документов юридического лица или доверенности;
- поле «Общее имя»* содержит фамилию, имя и отчество (если имеется) – в сертификате для физического лица, или полное наименование юридического лица, как оно указано в уставных документах, – в сертификате для юридического лица;
- поле «Фамилия»* содержит фамилию — Владельца сертификата для физического лица, или уполномоченного представителя, действующего от имени юридического лица, – в сертификате для юридического лица;
- поле «Приобретенное имя»* содержит имя и отчество (если имеется) — Владельца сертификата для физического лица, или уполномоченного представителя, действующего от имени юридического лица, – в сертификате для юридического лица;
- поле «СНИЛС»* содержит страховой номер индивидуального лицевого счета (11 десятичных цифр) — Владельца сертификата для физического лица, или уполномоченного представителя, действующего от имени юридического лица, – в сертификате для юридического лица;
- поле «ИНН»* содержит индивидуальный номер налогоплательщика — юридического лица в сертификате для юридического лица (12 десятичных цифр, включая 2 лидирующих нуля и 10 цифр ИНН юридического лица) или физического лица – в сертификате для физического лица или индивидуального предпринимателя (12 десятичных цифр);
- поле «ОГРН»* содержит основной государственный регистрационный номер юридического лица (13 десятичных цифр);
- поле «ОГРНИП» содержит основной государственный регистрационный номер индивидуального предпринимателя (15 десятичных цифр);
- поле «E-mail адрес» должно содержать адрес электронной почты Владельца сертификата.

2.8.2.2. Аутентификация Пользователя УЦ. Порядок установления личности

Начальная аутентификация физического лица производится с использованием документа, удостоверяющего личность. Порядок установления личности Заявителя приводится в п. 3.1.1.2 настоящего Регламента.

В том случае, если Пользователь УЦ является представителем (сотрудником) юридического лица (организации), его уникальное имя должно включать полное наименование данного юридического лица и должность. Для подтверждения этих данных представитель юридического лица при регистрации в УЦ, помимо удостоверения личности, должен предоставить официальный документ (доверенность), заверенный подписью руководителя и печатью организации, подтверждающий его принадлежность к данной организации, а также занимаемую им должность.

Удостоверяющие документы предоставляются в УЦ лично Заявителем.

2.8.3. Идентификация и аутентификация зарегистрированного Пользователя УЦ

2.8.3.1. Идентификация зарегистрированного Пользователя УЦ

Идентификация зарегистрированного Пользователя УЦ осуществляется по уникальному имени, занесенному в реестр Удостоверяющего центра при его первичной регистрации.

2.8.3.2. Аутентификация зарегистрированного Пользователя УЦ

Аутентификация зарегистрированного Пользователя УЦ может быть выполнена несколькими способами:

- очная аутентификация;

- удаленная аутентификация по ключевой фразе;
- удаленная аутентификация по сертификату.

Очная аутентификация Пользователя УЦ выполняется по паспорту или другому документу, удостоверяющему личность, предъявляемому лично.

Удаленная аутентификация по аварийному паролю (ключевой фразе) выполняется при обращении зарегистрированного Пользователя в УЦ (например, по телефону) с заявлением на аннулирование (отзыв) сертификата. Лицо, проходящее процедуру удаленной аутентификации, должно сообщить свои идентификационные данные и по запросу сотрудника УЦ назвать аварийный пароль. Аварийный пароль передается Пользователю при первичной регистрации и является одноразовой. Аварийный пароль действует на протяжении срока действия сертификата до окончания срока действия, либо аннулирования сертификата.

Удаленная аутентификация по сертификату ключа проверки ЭП зарегистрированного Пользователя УЦ осуществляется путем выполнения процедуры проверки электронной подписи Пользователя в представленном им электронном документе. Аутентификация по сертификату выполняется при удаленном обращении зарегистрированного Пользователя в УЦ с заявлениями на формирование или аннулирование (отзыв) сертификата, поданными в электронной форме с электронной подписью Пользователя, а также при проведении экспертных работ по подтверждению подлинности электронной подписи в электронном документе.

3. Порядок и сроки предоставления услуг Удостоверяющим центром

3.1. Порядок действий при первичной регистрации Пользователей УЦ, генерации ключей и изготовления сертификатов

Регистрация Пользователей УЦ – это внесение регистрационной информации о Пользователях УЦ в реестр Удостоверяющего центра.

Процедура первичной регистрации и последующего обслуживания Пользователя УЦ включает следующие этапы:

1. передача в УЦ заявления на регистрацию вместе с перечнем документов, указанных в п.3.1.1.3;
2. изготовление ключей ЭП Пользователя и формирование запроса на сертификат ключа проверки ЭП формата PKCS#10 (см. п.3.1.2);
3. передача в УЦ файла запроса на сертификат ключа проверки ЭП и его бумажной копии;
4. верификация удостоверяющих документов и регистрация в УЦ файла запроса на сертификат ключа проверки ЭП (см. п.3.1.3.1);
5. изготовление сертификата ключа проверки ЭП (см. п.3.1.3.2);
6. передача изготовленного сертификата ключа проверки ЭП Пользователю (см. п.3.1.3.3).

3.1.1. Порядок подачи документов на изготовление и выдачу сертификатов

Удостоверяющий центр «e-Notary» начинает процедуру изготовления сертификатов ключей проверки ЭП для **физических лиц**, **индивидуальных предпринимателей** и **юридических лиц** только в том случае, если лицо (Заявитель), обратившееся в УЦ с заявкой на получение счета для оплаты услуг УЦ (см.п.1.4) , присоединилось к Регламенту УЦ (см. п.1.3.3), ознакомилось с Договором публичной оферты (https://www.e-notary.ru/info/contracts_offer) на изготовление и обслуживание сертификатов Удостоверяющим центром «e-Notary» и оплатило услуги УЦ, связанные с изготовлением сертификата.

После оплаты услуг УЦ по изготовлению сертификата Заявитель или его представитель должны передать в УЦ заявление на изготовление и выдачу сертификата, оформленное должным образом (см. п.3.1.1.1), а также другие документы и сведения, указанные в п.3.1.1.3.

3.1.1.1. Требования к заявлению на изготовление и выдачу сертификата

Заявление на первичное изготовление и выдачу сертификата ключа проверки ЭП (далее – Заявление) оформляется в бумажном виде. Заявление должно быть заполнено по форме Приложения 3 (при заказе опциональной услуги формирования ключа ЭП Заявителя) или по форме Приложения 4 (при самостоятельном формировании Заявителем ключа ЭП и запроса на сертификат) настоящего Регламента и заверено собственноручной подписью Заявителя – физического лица, а для юридических лиц – еще дополнительно подписью руководителя и печатью организации Заявителя.

Заявление должно содержать следующую информацию:

при оформлении на физическое лицо, представляющее юридическое лицо:

- полное и сокращенное наименование юридического лица в соответствии с уставными документами;
- должность, фамилия, имя и отчество (если имеется) руководителя юридического лица, без сокращений;
- фамилия, имя и отчество (если имеется) Заявителя — физического лица, без сокращений;
- сведения о документе, удостоверяющем личность Заявителя (вид, серия, номер, кем и когда выдан документ);
- адрес электронной почты для контакта с Заявителем;
- адрес местонахождения юридического лица;
- субъект Российской Федерации, в котором зарегистрировано юридическое лицо;
- идентификационный номер налогоплательщика (ИНН) юридического лица;
- основной государственный регистрационный номер (ОГРН) юридического лица;
- страховой номер индивидуального лицевого счета (СНИЛС) представителя юридического лица;
- Данные доверенности или иных документов, подтверждающих правомочность действий от имени юридического лица;

при оформлении на физическое лицо или индивидуального предпринимателя:

- фамилия, имя и отчество (если имеется) Заявителя без сокращений;
- сведения о документе, удостоверяющем личность Заявителя (вид, серия, номер, кем и когда выдан документ);
- идентификационный номер налогоплательщика (ИНН) Заявителя;
- страховой номер индивидуального лицевого счета (СНИЛС) Заявителя;
- основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП) - только для индивидуального предпринимателя;
- адрес электронной почты для контакта с Заявителем.

В Заявлении также должно быть указано, что Заявитель выражает свое согласие на обработку предоставленных им персональных данных и гарантирует их достоверность.

Ответственность за полноту и достоверность информации, указанной в Заявлении, несет Заявитель.

Заявление может быть передано в Удостоверяющий центр как на бумажном носителе, так и в электронной форме. При подаче Заявления в электронной форме оно должно быть подписано квалифицированной электронной подписью Заявителя (если она у него есть) и может быть предоставлено в УЦ на электронном носителе при личном посещении УЦ Заявителем или его представителем.

Передача Заявления в электронной форме через Интернет возможна только в случае организации между Заявителем и УЦ надежного канала доставки, обеспечивающего конфиденциальность персональных данных в Заявлении.

3.1.1.2. Порядок установления личности Заявителя

Согласно №63-ФЗ «Об ЭП», при приеме заявления на изготовление и выдачу сертификата, а также при выдаче сертификата, сотрудники УЦ обязаны установить личность Заявителя или его представителя.

Установление личности Заявителя или его представителя производится в следующем порядке:

- личность гражданина Российской Федерации устанавливается по основному документу, удостоверяющему личность – паспорту гражданина Российской Федерации. В исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, удостоверяющий центр может удостоверить его личность по иному документу, удостоверяющему личность в соответствии с законодательством Российской Федерации;
- личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства; к документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами;
- личность беженца, вынужденного переселенца и лица без гражданства устанавливается на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц.

3.1.1.3. Перечень документов, запрашиваемых Удостоверяющим центром для изготовления и выдачи сертификата

При условии оплаты счета, для формирования ключей (опционально) и изготовления сертификата Заявителю необходимо подготовить и представить в УЦ следующие документы и сведения:

- Заявление о присоединении к Регламенту УЦ по форме Приложения 1 настоящего Регламента, заверенное собственноручной подписью Заявителя — для физических лиц, а для юридических лиц — подписью руководителя и печатью организации;
- Заявление на изготовление и выдачу сертификата ключа проверки ЭП по форме Приложения 3 (при заказе опциональной услуги формирования ключа ЭП Заявителя) или по форме Приложения 4 (при самостоятельном формировании Заявителем ключа ЭП и запроса на сертификат) настоящего Регламента, заверенное собственноручной подписью Заявителя — физического лица, а для юридических лиц – еще дополнительно подписью руководителя и печатью организации Заявителя;
- бумажную копию запроса на сертификат по форме Приложения 5 настоящего Регламента (при самостоятельном формировании Заявителем ключа ЭП и запроса на сертификат); ответственность за достоверность информации в запросе несет Заявитель;

- документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности (см. п. 3.1.1.2), а также другие документы и сведения, на основании которых УЦ вносит информацию в сертификат;

для физических лиц:

- основной документ, удостоверяющий личность Заявителя, на чье имя изготавливается сертификат (Владелец сертификата);
- страховой номер индивидуального лицевого счета (СНИЛС) Заявителя, на чье имя изготавливается сертификат;
- идентификационный номер налогоплательщика (ИНН) физического лица;
- если Заявитель является представителем другого физического лица, должен быть представлен оригинал доверенности или иной документ, подтверждающей право Заявителя действовать от имени этого физического лица;

для юридических лиц:

- полное и сокращенное наименование юридического лица в соответствии с уставными документами;
- основной документ, удостоверяющий личность Заявителя, на чье имя изготавливается сертификат (Владелец сертификата — физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности);
- основной государственный регистрационный номер (ОГРН) юридического лица;
- страховой номер индивидуального лицевого счета (СНИЛС) Заявителя, на чье имя изготавливается сертификат;
- оригинал или нотариально заверенная копия доверенности (по форме Приложения 2 настоящего Регламента) или иного документа, подтверждающего право Заявителя действовать от имени юридического лица и заверяющий его должностные полномочия в рамках своей организации; полномочия Заявителя действовать от имени юридического лица могут быть оформлены как приказ, выписка из приказа, письменное поручение, доверенность, письмо и т.п., заверенные печатью организации и подписью руководителя;
- копии документов, подтверждающих полномочия руководителя;

для индивидуальных предпринимателей:

- основной документ, удостоверяющий личность Заявителя, на чье имя изготавливается сертификат (Владелец сертификата);
- основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП), на чьё имя изготавливается сертификат;
- номер страхового свидетельства государственного пенсионного страхования (СНИЛС) Заявителя, на чье имя изготавливается сертификат.

Удостоверяющий центр вправе дополнительно запросить иные документы, подтверждающие все обстоятельства, сопутствующие уполномочию Заявителя, или необходимые для подтверждения сведений, включаемых в сертификат.

Допускается объединение заявления о присоединении к Регламенту с заявлением на изготовление и выдачу сертификата.

Удостоверяющий центр вправе отказать Заявителю в приеме документов в следующих случаях:

- если документы не соответствуют требованиям действующих нормативных правовых актов Российской Федерации;

- при ненадлежащем оформлении регистрационных документов;
- при наличии противоречий между сведениями, представленными Заявителем и сведениями, полученными Удостоверяющим центром из государственных информационных ресурсов в соответствии с частью 2.2 статьи 18 №63-ФЗ «Об ЭП».

Комплект указанных выше документов передается в УЦ при личном визите Заявителя в УЦ (см. п.3.1.3).

3.1.2. Процедура генерации ключей ЭП и запросов на сертификаты

В УЦ e-Notary допускаются следующие способы генерации ключа ЭП и запроса на сертификат:

1. самостоятельно, самим Заявителем, на своем рабочем месте; генерация ключа ЭП и запроса на сертификат выполняется в этом случае с помощью программного обеспечения, имеющегося у Заявителя или предоставленного ему после оплаты счета, согласно Заявке на поставку товаров и оказание услуг УЦ;
2. сотрудником УЦ, на специально оборудованном автоматизированном рабочем месте (АРМ), аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите информации, размещенном в аттестованном помещении УЦ;
3. самостоятельно, самим Заявителем, на специально оборудованном АРМ, аттестованном на соответствие требованиям законодательства Российской Федерации по технической защите информации, размещенном в аттестованном помещении УЦ.

Создание ключа ЭП и ключа проверки ЭП должно осуществляться Пользователем при помощи средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности, в соответствии с правилами пользования и руководством пользователя, входящими в комплект эксплуатационной документации на это средство.

3.1.2.1. Порядок генерации ключей ЭП на АРМ Заявителя

Если формирование ключа ЭП и запроса на сертификат Заявитель будет выполнять самостоятельно на своём рабочем месте, он должен приобрести (если у него нет) программное обеспечение (ПО) для генерации ключей и запросов на сертификаты, использующее средства ЭП, сертифицированные ФСБ России (например, программу «Admin-PKI», криптопровайдер «Signal-COM CSP», программу «KeyGen» и др.). Выбор конкретного ПО для генерации ключей и запросов на сертификат зависит от средства формирования электронной подписи, которое Заявитель в дальнейшем будет использовать в своей работе.

Передача Заявителю дистрибутивов оплаченного ПО должна осуществляться по надежным каналам доставки, одним из следующих способов:

1. при личном посещении Заявителем офиса УЦ;
2. через доставку курьером, службами экспресс-доставки, заказными бандеролями и др. в опечатанном и пронумерованном сейф-пакете; сейф-пакет опечатывается таким образом, что любая попытка его вскрытия не может остаться незамеченной;
3. путем загрузки дистрибутива ПО со страницы Портала УЦ, по каналу, защищенному протоколом TLS с использованием стандартных средств браузера, с обязательным последующим выполнением процедуры контроля целостности ПО с помощью сертифицированной ФСБ России утилиты для вычисления хэш и эталонной контрольной суммы, которые Заявитель получает по другим каналам.

При первичной регистрации Заявителя в УЦ в качестве канала надежной доставки ПО, как правило, используются варианты 1) или 2).

При *самостоятельном* выполнении процедуры генерации ключей и запросов на своем рабочем месте Заявитель должен выполнить следующую последовательность действий:

- с помощью ПО для генерации ключей и запросов на сертификат сформировать ключ ЭП на отчуждаемый ключевой носитель, поддерживаемый данным ПО и разрешенный к использованию (Рутокен, Рутокен ЭЦП 2.0, JaCarta PKI, JaCarta GOST, USB Hard Flash Drive и др.), и файл самоподписанного запроса на сертификат формата PKCS#10 (запрос, подписанный ключом ЭП, парным ключу проверки ЭП, включенному в запрос);
- средствами ПО для генерации ключей и запросов на сертификат распечатать запрос на сертификат и заверить его бумажную копию собственноручной подписью, а для юридических лиц – дополнительно подписью руководителя и печатью организации Заявителя;
- электронную форму запроса на сертификат передать в УЦ лично или послать по электронной почте;
- бумажную копию запроса передать в УЦ лично, курьерской связью или заверить у нотариуса и послать по почте вместе с остальными документами (см. п. 3.1.1.3).

В случае самостоятельного создания ключа ЭП Заявитель должен подтвердить владение ключом ЭП, соответствующим ключу проверки ЭП в составе файла запроса на сертификат, переданном им при обращении в УЦ вместе с Заявлением на изготовление и выдачу сертификата. Подтверждение владения ключом ЭП выполняется средствами УЦ путем проверки электронной подписи в предоставленном Заявителем файле запроса на сертификат формата PKCS#10. При отрицательном результате проверки электронной подписи в файле запроса на сертификат УЦ отказывает заявителю в изготовлении и выдаче сертификата.

3.1.2.2. Порядок генерации ключей ЭП на АРМ Удостоверяющего центра

По обращению Заявителя сотрудник УЦ выполняет формирование ключа ЭП и запроса на сертификат в соответствии со следующими положениями настоящего Регламента:

- формирование ключа ЭП и запроса на сертификат выполняется сотрудником УЦ на основании принятого Заявления, в присутствии Заявителя, на аттестованном АРМ, размещенном на территории УЦ;
- сформированный ключ ЭП записывается на отчуждаемый ключевой носитель, предоставленный Заявителям или приобретенный в УЦ;
- отчуждаемый ключевой носитель должен удовлетворять следующим требованиям:
  - входить в перечень разрешенных к использованию устройств;
  - быть проинициализированным (отформатированным);
  - не содержать никакой информации, за исключением данных инициализации;
- ключевые носители, не удовлетворяющие указанным требованиям, для записи на них ключевой информации не принимаются;
- ключевой носитель, содержащий изготовленный ключ ЭП, передается лично Заявителю (Владельцу) либо доверенному лицу Заявителя; факт выдачи ключей заносится в Журнал учета изготовления и выдачи ключей и заверяется собственноручной подписью Заявителя (Владельца) либо его доверенным лицом.

Действия Заявителя при самостоятельном выполнении процедуры генерации ключей на АРМ в Удостоверяющем центре аналогичны действия сотрудника УЦ и выполняются под его контролем.

Файл запроса на сертификат, доставленный Заявителем или сформированный уполномоченным сотрудником УЦ, экспортируется в УЦ.

3.1.3. Порядок изготовления и выдачи сертификата при личном обращении Заявителя

3.1.3.1. Порядок проверки документов и сведений

Если комплект документов и сведений, указанных в п.3.1.1.3 настоящего Регламента, передается в УЦ при личном визите Заявителя, сотрудник УЦ устанавливает личность Заявителя и проверяет достоверность представленной информации:

- с учетом положений п.3.1.1.2 настоящего Регламента идентифицируется личность Заявителя – физического лица по паспорту или иному документу, удостоверяющему личность, и проверяются полномочия физического лица, выступающего от имени Заявителя – юридического лица;
- проверяется соответствие персональных данных, указанных в Заявлении на изготовление и выдачу сертификата, представленным данным удостоверения личности или заверенным сведениям;
- для подтверждения достоверности документов и сведений, представленных Заявителем для включения в сертификат, из государственных информационных ресурсов запрашивается:
  - выписка из единого государственного реестра юридических лиц в отношении заявителя — юридического лица;
  - выписка из единого государственного реестра индивидуальных предпринимателей в отношении заявителя — индивидуального предпринимателя;
  - выписка из единого государственного реестра налогоплательщиков в отношении заявителя — иностранной организации;
- если полученные из государственных реестров сведения подтверждают достоверность информации, представленной Заявителем, принимается решение о регистрации Заявителя в УЦ и регистрационная информация заносится в реестр УЦ;
- если генерация ключа ЭП и формирование запроса на сертификат выполнялись Заявителем самостоятельно, проверяется:
  - соответствие запроса сертификата, полученного в электронном виде, представленной бумажной копии;
  - соответствие персональных данных, указанных в запросе, представленным данным удостоверения личности или заверенным сведениям, и при их совпадении бумажная копия запроса заверяется собственноручной подписью уполномоченного сотрудника УЦ и печатью УЦ.

В случае неполноты или неподтверждения достоверности данных, представленных Заявителем, сотрудник УЦ отказывает в регистрации Заявителя и изготовлении сертификата и возвращает Заявителю документы с указанием причины отказа. В этом случае Заявитель должен сформировать новый комплект документов и повторно обратиться в УЦ.

3.1.3.2. Порядок изготовления сертификата

В случае принятия положительного решения о регистрации Заявителя и изготовлении сертификата, сотрудник УЦ формирует для него ключ ЭП (опционально) в соответствии с положениями п.3.1.2.2 настоящего Регламента и передает на сертификацию в ПАК УЦ файл запроса на сертификат, сформированный им самим или доставленный Заявителем (при самостоятельной генерации ключа ЭП и запроса на сертификат Заявителем).

На основании поступившего файла запроса на сертификат, УЦ изготавливает сертификат ключа проверки ЭП в электронной форме, автоматически помещает его в сетевой Справочник сертификатов УЦ и уведомляет Заявителя об изготовлении сертификата по адресу электронной почты, включенному в состав соответствующего сертификата.

Уполномоченный сотрудник УЦ распечатывает на бумажном носителе две копии изготовленного сертификата и заверяет их собственноручной подписью и печатью УЦ.

Изготовление сертификата ключа ЭП (опционально) и сертификата ключа проверки ЭП может быть выполнено в день личного посещения офиса УЦ Заявителем, при условии предварительной оплаты счета на оказание услуг УЦ и корректно подготовленных документов и сведений, необходимых для изготовления сертификата. День и время посещения УЦ должно быть заранее согласовано с уполномоченным сотрудником УЦ.

3.1.3.3. Порядок выдачи сертификата

Выдача изготовленного сертификата осуществляется при личном посещении Удостоверяющего центра Заявителем и только после установления личности в соответствии с положением п.3.1.1.2 настоящего Регламента.

Для ознакомления с информацией, содержащейся в сертификате, Заявителю при выдаче сертификата предоставляется его бумажная копия в двух экземплярах. Обе копии сертификата на бумажном носителе заверяются собственноручной подписью Заявителя, подтверждающей корректность сведений, указанных в сертификате. Один экземпляр бумажной копии сертификата остается в УЦ, а второй передается Заявителю.

По окончании процедуры изготовления сертификата Заявителю выдаются:

- ключ ЭП, записанные на отчуждаемый ключевой носитель (если его генерация выполнялась сотрудником УЦ);
- сертификат ключа проверки ЭП Заявителя в электронной форме, соответствующий его ключу ЭП;
- копия сертификата ключа проверки ЭП Заявителя на бумажном носителе, заверенная обеими сторонами — собственноручной подписью Заявителя и подписью уполномоченного сотрудника УЦ;
- предоставляется Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи, а также иных инструкций по работе со средствами криптографической защиты информации и информационной безопасности (Приложения 8 настоящего Регламента);
- сертификат УЦ в электронной форме или ссылка на ресурс, где опубликованы сертификаты УЦ e-Notary (см. п.2.3.1);
- копия сертификата УЦ на бумажном носителе, заверенная собственноручной подписью уполномоченного сотрудника УЦ (по запросу Заявителя);
- полный комплект бухгалтерских документов по оплаченному счету;
- аварийный пароль в запечатанном виде для удаленной аутентификации: используется для связи с УЦ по телефону на случай нештатных ситуаций (компрометация ключей, отзыв сертификата и др.) и должен храниться у пользователя наравне с ключами.

Электронные формы сертификатов ключей проверки ЭП Заявителя и УЦ передаются Заявителю в виде файлов, записанных на CD-диск или на отчуждаемый ключевой носитель (если это позволяет тип носителя).

При приобретении Заявителем лицензии на программное обеспечение, необходимое для его дальнейшей работы с защищенными информационными системами и системами электронного документооборота, дистрибутив данного программного обеспечения записывается на CD-диск, содержащий электронные формы сертификатов ключей проверки ЭП Заявителя и УЦ.

3.1.3.4. Срок создания и выдачи сертификата

Создание и выдача квалифицированного сертификата осуществляется Удостоверяющим центром в течение не более двух рабочих дней со дня получения необходимых документов, оплаты и идентификации Заявителя.

В случае необходимости создания и выдачи квалифицированного сертификата в течение дня Заявитель должен произвести дополнительную оплату срочного изготовления сертификата и представить в Удостоверяющий центр платежное поручение с отметкой банка о том, что платеж произведен.

3.2. Порядок действий при проведении плановой смены ключей ЭП и обновлении сертификатов Пользователей УЦ

Не позднее, чем за 2 (две) недели до окончания периода действия текущего рабочего ключа ЭП, Владелец сертификата (Заявитель) должен обратиться в УЦ e-Notary за формированием нового ключа ЭП (опционально) и сертификата ключа проверки ЭП. Наличие одновременно двух рабочих сертификатов с перекрывающимися сроками действия обеспечивает Владельцу в период проведения плановой смены ключей возможность непрерывной работы с защищенными сервисами, выполняя формирование ЭП на новом ключе, а расшифрование адресованной ему информации – на старом и новом.

Обновление сертификатов ключей проверки ЭП для физических лиц, индивидуальных предпринимателей и юридических лиц осуществляется только после оплаты счета на оказание услуг по формированию ключа ЭП (опционально) и изготовлению сертификата, на основании заключенного ранее Договора публичной оферты на изготовление и обслуживание сертификатов в УЦ e-Notary и Заявления на изготовление сертификата зарегистрированного Владельца по форме Приложения 3 (при заказе опциональной услуги формирования ключа ЭП) или по форме Приложения 4 (при самостоятельном формировании Заявителем ключа ЭП и запроса на сертификат) настоящего Регламента.

Заявка для получения счета на оплату услуг УЦ по обновлению сертификата формируется одним из способов, указанных в п.1.4 настоящего Регламента.

При изготовлении ключа ЭП самим Заявителем или сотрудником УЦ на АРМ, установленном в офисе Удостоверяющего центра (см. п. 3.1.2.2), дальнейший порядок действий Заявителя при проведении плановой смены ключа ЭП и сертификата соответствует порядку действий при первичном изготовлении сертификата на основании электронной формы запроса на сертификат формата PKCS#10 (см. п. 3.1.3.2).

При самостоятельном изготовлении новых ключей ЭП и запроса на обновление сертификата (по Заявлению, согласно Приложения 4 настоящего Регламента) Заявитель может подать в УЦ Заявление на изготовление и выдачу сертификата как на бумажном носителе, так и в электронной форме в виде сформированного запроса на сертификат формата CMC: запрос формата PKCS#10 с новым ключом проверки ЭП Заявителя, подписанный его действующим ключом ЭП. Формирование запросов формата CMC обеспечивается программами Admin-PKI v5, KeyGen и средствами Web-интерфейса УЦ e-Notary разработки АО «СИГНАЛ-КОМ».

Если к моменту плановой смены ключей атрибуты Заявителя, включаемые в состав нового сертификата, не изменились и совпадают с атрибутами действующего сертификата, запрос формата CMC на обновление сертификата передается в УЦ без необходимости передачи подтверждающих документов в бумажном виде. Документы, подтверждающие полномочия лица, являющегося представителем Заявителя, предоставляются в УЦ в том же объеме, что и при первичной регистрации в УЦ.

При изменении атрибутов в запросе на новый сертификат изготовление сертификата производится в соответствии с п. 3.1 настоящего Регламента, но без первичной регистрации в УЦ.

Об изготовлении нового сертификата Заявитель уведомляется по адресу электронной почты, включенному в состав сертификата.

По ссылке, полученной вместе с уведомлением об изготовлении сертификата, Заявитель скачивает свой сертификат и сертификат УЦ. Собственный сертификат может быть сохранен на компьютере, а сертификат УЦ рекомендуется хранить на секретном ключевом носителе. С момента получения сертификата ключа проверки ЭП ключевой носитель с соответствующим ключом ЭП становится рабочим ключевым носителем.

Полный комплект бухгалтерских документов по оплаченному счету высылается Заявителю по почте.

Ключевые носители с ключами ЭП, срок действия которых истек, должны уничтожаться путем переформатирования.

3.3. Внеплановая смена ключей зарегистрированного Пользователя УЦ

Внеплановая смена ключа ЭП и обновление сертификата ключа проверки ЭП осуществляются Пользователем УЦ в следующих случаях:

- если Пользователь УЦ не успел обновить сертификат ключа ЭП до истечения периода его действия;
- при компрометации ключа ЭП Пользователя УЦ (см.п.3.5.3);
- при компрометации ключа ЭП Удостоверяющего центра (см. п.3.6.2);
- в случае иных форс-мажорных обстоятельств.

Процедуру внеплановой смены ключа ЭП по указанным выше обстоятельствам Пользователь УЦ осуществляет после оплаты счета, в соответствии с порядком, установленным в п.3.1 настоящего Регламента, но без первичной регистрации в УЦ.

3.5. Аннулирование (отзыв) сертификата Пользователя УЦ

Аннулирование (отзыв) сертификата Пользователя УЦ осуществляется в следующих случаях (подробнее см. п.3.5.2):

- по решению администрации УЦ;
- по заявлению Владельца сертификата;
- указанию лиц или органов, имеющих такое право в силу закона;
- по заявлению Стороны (присоединившийся Регламенту в качестве юридического лица) на отзыв доверенности своего представителя, зарегистрированного в УЦ.

При аннулировании (отзыве) сертификата заявитель должен указывать следующие сведения:

- серийный номер отзываемого сертификата;
- причину отзыва сертификата (см. п.6.2.3).

3.5.1. Основания для прекращения действия или аннулирования сертификата Пользователя УЦ

В УЦ e-Notary сертификат Пользователя УЦ (Владельца) изымается из обращения (отзывается или аннулируется) в следующих случаях:

- при компрометации ключей ЭП Владельца (см. п.3.5.3);
- в случае изменения атрибутов в сертификате, по заявлению Владельца сертификата в письменной форме, а для юридических лиц – по заявлению, заверенному руководителем и печатью организации Владельца;
- при обнаружении администрацией УЦ факта изменения атрибутов в сертификате Владельца;
- в случае заявления Владельца о прекращении Договора на обслуживание в УЦ;
- при отзыве доверенности, на основании которой был выдан сертификат уполномоченному представителю Стороны, присоединившейся к Регламенту;
- в случае прекращения деятельности УЦ без передачи его функций другим лицам;
- если не подтверждено, что Владелец сертификата владеет ключом ЭП, соответствующим ключу проверки ЭП, указанному в сертификате;
- если установлено, что содержащийся в сертификате ключ проверки ЭП уже содержится в ином ранее созданном сертификате;
- если вступило в силу решение суда, которым установлено, что сертификат содержит недостоверную информацию.

Отзыв сертификатов Владельца может также осуществляться по инициативе администрации УЦ в случаях истечения одного из следующих сроков:

- срока полномочий Владельца;
- срока действия иного документа, на основании которого был оформлен сертификат Владельца.

3.5.2. Порядок действия УЦ при аннулировании (отзыве) сертификата Пользователя УЦ

В случае аннулировании (отзыва) сертификата **по инициативе УЦ** уполномоченный сотрудник УЦ помещает его серийный номер в Список отозванных сертификатов (СОС) с указанием причины отзыва и публикует СОС в сетевом Справочнике сертификатов УЦ.

При отзыве сертификата **по инициативе Владельца** заявление на аннулирование (отзыв) сертификата подаётся Владельцем в бумажной, устной или электронной форме:

- заявление на аннулирование (отзыв) сертификата *в бумажной форме* заполняется по образцу Приложения 6 настоящего Регламента и подаётся Владельцем сертификата в УЦ лично, заказным письмом или курьерской связью.
- заявление на аннулирование (отзыв) сертификата *в устной форме* подаётся Владельцем сертификата в УЦ посредством телефонной связи, с указанием аварийного пароля, полученного при первичной регистрации; впоследствии Владелец сертификата должен предоставить в УЦ заявление об аннулировании (отзыве) сертификата по форме Приложения 6 настоящего Регламента;
- заявление на аннулирование (отзыв) сертификата *в электронной форме* подаётся Владельцем сертификата в УЦ по электронной почте с помощью заявки на отзыв сертификата, подписанной действующим ключом ЭП.

Аннулирование (отзыв) сертификата Владельца, являющегося полномочным представителем Стороны, присоединившийся к Регламенту, осуществляется **путём отзыва доверенности**, на основании которой предоставлялись услуги УЦ. Форма заявления об отзыве доверенности приведена в Приложении 7 настоящего Регламента.

Обработка заявления на отзыв сертификата, выпуск и публикация СОС в сетевом Справочнике сертификатов УЦ и в точках распространения СОС, указанных в расширении CDP

(CRLDistributionPoint) сертификатов, а также уведомление Владельца об аннулировании (отзыве) сертификата ключа ЭП, должны быть осуществлены не позднее двенадцати часов с момента наступления обстоятельств, указанных в п. 3.5.1 настоящего Регламента, или с момента, когда Удостоверяющему центру стало известно о наступлении таких обстоятельств.

Дата, с которой сертификат считается недействительным, устанавливается равной дате формирования СОС, в который был включен серийный номер отозванного сертификата.

Сертификаты с истекшим периодом действия не заносятся в СОС, т.к. криптографические приложения автоматически прекращают действия с просроченными сертификатами.

3.5.3. Порядок действий Пользователя УЦ при компрометации ключей ЭП

Пользователь Удостоверяющего центра (юридическое или физическое лицо) самостоятельно принимает решение о факте или угрозе компрометации своего ключа ЭП.

К событиям, на основании которых Владелец сертификата принимает решение о компрометации своего ключа ЭП, относятся, включая, но, не ограничиваясь, следующие:

- утрата ключевых носителей;
- утрата ключевых носителей с последующим обнаружением;
- для юридических лиц: увольнение сотрудников, имевших доступ к ключевым носителям;
- возникновение подозрений на утечку информации или ее искажение при работе в защищенном сервисе;
- нарушение правил хранения ключевых носителей.

В случае компрометации или угрозы компрометации ключа ЭП Пользователь прекращает его использование, для оперативности связывается с Удостоверяющим центром по телефону и в устной форме просит приостановить действие сертификата, соответствующего скомпрометированному ключу.

Получив от Владельца сертификата в устной форме сообщение о компрометации ключа ЭП (или подозрении на компрометацию), сотрудник УЦ в течение 2 (двух) часов должен связаться с ним по телефону или электронной почте для подтверждения факта компрометации. Если Владелец подтверждает компрометацию своих ключей устно или присылает заявление на отзыв сертификата в бумажной или электронной форме, сотрудник УЦ помещает соответствующий сертификат в Список отозванных сертификатов (СОС) с указанием причины «Компрометация ключа» и публикует СОС в сетевом Справочнике сертификатов.

Процедуру внеплановой смены скомпрометированных ключей Владелец осуществляет после оплаты счета, в соответствии с порядком, установленным в п.3.3 настоящего Регламента.

3.6. Порядок действий при смене ключей ЭП Удостоверяющего Центра

Порядок обновления ключей и сертификатов УЦ выполняется в соответствии с внутренним регламентом Удостоверяющего центра.

Новые сертификаты УЦ размещаются в сетевом Справочнике сертификатов УЦ, доступном всем Пользователям сертификатов.

3.6.1. Плановая смена ключей ЭП Удостоверяющего центра

Плановая смена ключей ЭП Удостоверяющего центра выполняется не позднее, истечения срока действия ключа ЭП УЦ или не менее чем за 1 год до окончания периода действия его сертификата ключа проверки ЭП.

Процедура плановой смены ключей УЦ осуществляется в следующем порядке:

- Администратор УЦ формирует для Удостоверяющего центра новый ключ ЭП и соответствующий ему сертификат ключа проверки ЭП;
- Уполномоченное лицо направляет в Головной удостоверяющий центр запрос на новый квалифицированный сертификат ключа проверки электронной подписи Удостоверяющего центра;
- После получения из Головного удостоверяющего центра нового квалифицированного сертификата подписи УЦ осуществляет информирование об этом Пользователей путем публикации нового квалифицированного сертификата в сетевом Справочнике сертификатов УЦ и доводит до всех Пользователей УЦ по надежному каналу сетевого взаимодействия;
- до окончания срока действия текущего ключа ЭП Удостоверяющего центра Пользователи УЦ должны получить новый сертификат УЦ и добавить его в справочники сертификатов, не удаляя действующий сертификат УЦ;
- старый ключ ЭП Удостоверяющего центра используется в течение своего срока действия для формирования СОС, изданных Удостоверяющим центром в период действия его старого ключа ЭП.

Плановая смена ключа электронной подписи УЦ не влечет за собой необходимости смены ключей электронных подписей и соответствующих квалифицированных сертификатов ключей проверки электронных подписей Пользователей.

3.6.2. Компрометация ключей ЭП Удостоверяющего центра

В случае компрометации ключа ЭП Удостоверяющего центра выполняется аннулирование (отзыв) соответствующего сертификата УЦ.

Информация о факте компрометации ключей Удостоверяющего центра размещается на страницах Web-ресурса УЦ http://www.e-notary.ru, а Пользователи УЦ оповещаются о компрометации путем соответствующей рассылки по электронной почте.

Процедура внеплановой смены скомпрометированных ключей Удостоверяющего центра осуществляется в соответствии с порядком, установленным в п. 3.6.1 настоящего Регламента для процедуры плановой смены ключей УЦ.

Все действующие (на момент компрометации), а также приостановленные, сертификаты ключей Пользователей УЦ, подписанные с использованием скомпрометированного ключа ЭП Удостоверяющего центра, считаются аннулированными (отозванными) и подлежат внеплановой смене на безвозмездной основе. Процедура внеплановой смены ключей Пользователей УЦ осуществляется в соответствии с порядком, установленным в п.3.3 настоящего Регламента.

3.7. Смена ключей оператора Регистрационного центра

Порядок обновления ключей и сертификатов Операторов РЦ выполняется в соответствии с внутренним регламентом УЦ e-Notary.

Новые сертификаты Операторов РЦ размещаются в сетевом Справочнике сертификатов УЦ, доступном всем Пользователям сертификатов (см. п.2.1.3).

3.7.1. Плановая смена ключей Оператора Регистрационного центра

Плановая смена ключей Оператора Регистрационного центра выполняется за 10 дней до окончания периода действия текущего сертификата Оператора РЦ.

Процедура плановой смены ключей Оператора РЦ осуществляется в следующем порядке:

- Оператор РЦ формирует новый ключ ЭП и импортирует файл запроса сертификата в УЦ по каналу защищенного взаимодействия между РЦ и УЦ;
- бумажная копия запроса на сертификат передается лично Оператором РЦ в УЦ;
- после сверки бумажной копии запроса и его электронной формы, а также идентификации личности, администратор Удостоверяющего центра изготавливает сертификат нового ключа проверки ЭП Оператора РЦ и регистрирует его в настройках УЦ в качестве параметра аутентификации данного Оператора;
- Оператор РЦ перегружает Регистрационный центр, используя для удаленного защищенного доступа к УЦ новые ключи и сертификат.

3.7.2. Компрометации ключевых документов Оператора Регистрационного центра

В случае компрометации ключа ЭП Оператора РЦ администратор УЦ выполняет аннулирование (отзыв) соответствующего сертификата, путем его занесения в Список отозванных сертификатов.

Процедуру внеплановой смены скомпрометированных ключей Оператор Регистрационного центра осуществляет в соответствии с порядком, установленным в п. 3.7.1 настоящего Регламента для процедуры плановой смены ключей Оператора РЦ.

3.8. Процедура подтверждения электронной подписи с использованием сертификата ключа проверки ЭП

По желанию Стороны, присоединившейся к Регламенту, Удостоверяющий центр выполняет процедуру подтверждения подлинности электронной подписи в электронном документе, представленном на экспертизу.

Подтверждение электронной подписи под электронным документом осуществляется Удостоверяющим центром после заключения договора на выполнение экспертных работ, составленного на основании заявления, поданного в простой письменной форме.

Заявление на подтверждение электронной подписи под электронным документом должно содержать информацию о дате и времени формирования электронной подписи.

При отсутствии штампа времени в электронной подписи доказательство достоверности даты и времени ее формирования под электронным документом возлагается на заявителя.

В качестве обязательного приложения к заявлению на подтверждение электронной подписи под электронным документом должны прилагаться следующие файлы:

- файл, содержащий подписанный электронной подписью документ формата CMS, или два файла, один из которых содержит документ, а другой — значение электронной подписи этого документа формата CMS;
- файл сертификата ключа проверки ЭП, с использованием которого необходимо проверить подлинность электронной подписи в электронном документе;
- файл сертификата ключа проверки ЭП Удостоверяющего центра, являющегося издателем сертификата ключа проверки ЭП автора электронной подписи;

- файл, содержащий СОС Удостоверяющего центра, являющегося издателем сертификата ключа проверки ЭП автора электронной подписи.

Срок рассмотрения заявления на подтверждение электронной подписи под электронным документом составляет 10 (Десять) рабочих дней с момента поступления в УЦ заявления и всех необходимых данных при условии поступления оплаты стоимости данной услуги на расчетный счет УЦ.

В случае отказа в выполнении экспертных работ по подтверждению электронной подписи под электронным документом заявителю возвращается заявление на подтверждение электронной подписи с резолюцией ответственного сотрудника Удостоверяющего центра.

В случае принятия положительного решения по заявлению, после проведения экспертной процедуры заявитель получает документ в письменной форме, заверенный собственноручной подписью ответственного сотрудника Удостоверяющего центра и печатью Удостоверяющего центра.

Заключение содержит следующую информацию:

- результат проверки электронной подписи под электронным документом, выполненной при помощи АРМ разбора конфликтных ситуаций «Arbiter-PKI»;
- детальный отчет по выполненной проверке.

Детальный отчет по выполненной проверке включает следующую информацию:

- время и место проведения экспертизы;
- основания для проведения экспертизы;
- сведения об эксперте или экспертной комиссии, которой поручено проведение экспертизы;
- объекты исследований и материалы по заявлению, представленные на экспертизу;
- содержание и результаты исследований;
- выводы по проведенной экспертизе.

Процедура подтверждения подлинности электронной подписи в электронном документе включает процедуру проверки действительности всех сертификатов, включенных в цепочку проверки сертификата, представленного на экспертизу, до сертификата аккредитованного УЦ, выданного головным Удостоверяющим центром — в случае проверки квалифицированной ЭП, или до корневого сертификата УЦ, обслуживающего неквалифицированные сертификаты — в случае проверки усиленной неквалифицированной ЭП.

Материалы и документы, иллюстрирующие заключение эксперта или комиссии экспертов, прилагаются к детальному отчету и служат его составной частью.

Детальный отчет составляется в простой письменной форме и заверяется собственноручной подписью эксперта или членами комиссии экспертов.

Стоимость услуги подтверждения подлинности электронной подписи в электронном документе размещается на портале УЦ e-Notary по адресу: http://www.e-notary.ru.

3.9. Порядок ведения реестра квалифицированных сертификатов (Справочника сертификатов)

Справочник сертификатов ведется УЦ в электронной форме в соответствии с требованиями, установленными согласно №63-ФЗ «Об ЭП», и кроме информации, содержащейся в

квалифицированных сертификатах, включает также информацию о датах прекращения действия или аннулирования квалифицированных сертификатов и об основаниях прекращения действия или аннулирования, а также иную информацию, подлежащую включению в реестр в соответствии с требованиями нормативных правовых документов.

УЦ обязан внести информацию о созданном квалифицированном в Справочник сертификатов не позднее одних суток с указанной в нем даты начала действия такого сертификата.

УЦ обязан внести информацию о квалифицированном сертификате, который был аннулирован или действие которого было досрочно прекращено, в Справочник сертификатов в течение 12 часов с момента возникновения обстоятельств, послуживших основанием для аннулирования или прекращения действия квалифицированного сертификата или в течение двенадцати часов с момента, когда УЦ стало известно или должно было стать известно о наступлении таких обстоятельств.

3.10. Порядок обслуживания реестра квалифицированных сертификатов (Справочника сертификатов)

Техническое обслуживание Справочника сертификатов осуществляется, как правило, в нерабочее время и не может превышать 3 (трех) часов.

УЦ осуществляет заблаговременное оповещение о планируемом проведении технического обслуживания Справочника сертификатов путем публикации соответствующей информации на портале УЦ e-Notary по адресу: http://www.e-notary.ru.

4. Порядок исполнения обязанностей Удостоверяющего центра

4.1. Информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки

Удостоверяющий центр осуществляет информирование Заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, путем включения этой информации в предоставляемое каждому получателю квалифицированного сертификата руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи (см. п.7 Регламента и Приложение 8).

Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, содержащее указанную информацию, публикуется также на сайте Удостоверяющего центра.

4.2. Выдача по обращению Заявителя средств электронной подписи

Средства электронной подписи, выдаваемые УЦ Заявителю, должны иметь подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи».

Выдача по обращению Заявителя средств электронной подписи осуществляется путем поставки средств криптографической защиты способом, определенным эксплуатационной документацией на эти средства.

4.3. Обеспечение актуальности информации, содержащейся в реестре квалифицированных сертификатов, и ее защиты от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий

Актуальность информации, содержащейся в реестре квалифицированных сертификатов, обеспечивается путем выполнения УЦ порядка ведения Справочника сертификатов (см. п.3.9), а также защиты указанной информации от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий.

Защита информации, содержащейся в Справочнике сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий обеспечивается комплексом организационно-технических мероприятий, осуществляемых УЦ в соответствии с требованиями, установленными эксплуатационной документацией на средства удостоверяющего центра, а также требованиями, установленными в области технической защиты информации.

4.4. Обеспечение доступности Спровочника сертификатов в информационно-телекоммуникационной сети «Интернет»

Информация, содержащаяся в Справочнике сертификатов УЦ, доступна любому лицу в любое время, за исключением периодов технического обслуживания реестра квалифицированных сертификатов, по портале УЦ e-Notary по адресу: https://www.e-notary.ru/services.

4.5. Порядок обеспечения конфиденциальности созданных Удостоверяющим центром ключей электронных подписей

Конфиденциальность созданных Удостоверяющим центром ключей электронных подписей обеспечивается комплексом организационно-технических мероприятий, осуществляемых УЦ в соответствии с требованиями, установленными:

- эксплуатационной документацией на средства удостоверяющего центра и средства электронной подписи;
- нормативными документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, в отношении безопасности информации автоматизированных систем, предназначенных для хранения и обработки конфиденциальной информации;
- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152.

Временное хранение ключей электронных подписей, созданных Удостоверяющим центром по обращению Заявителей, осуществляется в соответствии с требованиями, установленными настоящим регламентом, эксплуатационной документации на средства УЦ и средства ЭП, а также действующим законодательстом.

Временное хранение ключей электронных подписей, созданных Удостоверяющим центром по обращению Заявителей, осуществляется в течение не более 2 (двух) дней с момента их создания. В

случае неполучения Заявителями созданных по их обращениям ключей электронной подписи до истечения указанного срока ключи электронной подписи уничтожаются УЦ.

Удостоверяющий центр не осуществляет депонирование и (или) архивирование ключей электронных подписей Пользователей.

4.6. Регистрация квалифицированного сертификата в Единой системе идентификации и аутентификации

В соответствии с требованиями части 5 статьи 18 №63-ФЗ «Об ЭП» при выдаче квалифицированного сертификата УЦ направляет в Единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в Единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра).

4.7. Регистрация владельца квалифицированного сертификата в Единой системе идентификации и аутентификации

УЦ осуществляет регистрацию физического лица в Единой системе идентификации и аутентификации на основании заявления, поданного в Удостоверяющий центр в форме документа на бумажном носителе с собственноручной подписью владельца сертификата.

УЦ осуществляет регистрацию в Единой системе идентификации и аутентификации как физических лиц, являющихся Владельцами выданных УЦ квалифицированных сертификатов, так и физических лиц, имеющих право действовать от имени юридического лица без доверенности и указанных в качестве Владельца квалифицированного сертификата наряду с наименованием юридического лица, которому был выдан сертификат.

Регистрация в Единой системе идентификации и аутентификации юридических лиц осуществляется самостоятельно физическими лицами, имеющими право действовать от имени юридического лица без доверенности, после прохождения ими процедуры регистрации в Единой системе идентификации и аутентификации в качестве физических лиц.

4.8. Предоставление доступа к информации, содержащейся в реестре квалифицированных сертификатов

Доступ к информации, содержащейся в Справочнике сертификатов, включая информацию об аннулировании (отзыве) квалифицированного сертификата, предоставляется безвозмездно любому лицу в соответствии с порядком, указанным в пункте 4.4 настоящего Регламента.

5. Дополнительные положения

5.1. Требования к средствам электронной подписи Пользователей УЦ

Средство электронной подписи должно обеспечивать выполнение следующих процедур:

- генерацию ключей ЭП и ключей проверки ЭП;
- формирование электронной подписи;
- проверку электронной подписи.

Средство электронной подписи должно обеспечивать выполнение мер защиты ключей ЭП (см. п. 7 и Приложение 8).

В качестве средства электронной подписи Пользователи должны использовать ПО, разработанное с использованием сертифицированных в соответствии с правилами сертификации средств криптографической защиты информации по уровню защиты КС1, КС2.

Идентификаторы алгоритмов должны быть зарегистрированы в настоящем Регламенте в п.6.

5.2. Сроки действия ключей ЭП и сертификатов ключей проверки ЭП

Сроки действия ключа ЭП и соответствующего сертификата ключа проверки ЭП Пользователя УЦ определяются в соответствии с эксплуатационной документацией средства ЭП, которое использовалось при генерации ключа ЭП:

- максимальный срок действия ключа ЭП — 1 год и 3 месяца;
- максимальный срок действия сертификата ключа проверки ЭП не может превышать срока действия соответствующего ключа ЭП более, чем на 15 лет.

В соответствии с настоящим Регаментом срок действия ключа проверки ЭП устанавливается равным сроку действия сертификата ключа проверки ЭП и составляет 1 год.

Начало периода действия ключа ЭП Пользователя УЦ исчисляется с даты и времени начала действия соответствующего сертификата ключа проверки ЭП Пользователя УЦ.

Срок действия сертификата ключа проверки ЭП Пользователя УЦ устанавливается Удостоверяющим центром в момент его изготовления.

Конец периода действия сертификата пользователя задается в соответствии с требованиями регламента работы сети конфиденциальной связи и автоматически ограничивается периодом действия рабочего сертификата УЦ.

Период времени действия ключа ЭП, соответствующего выданному сертификату ключа проверки ЭП Пользователя УЦ должен находиться в пределах периода времени, на который Стороной, присоединившейся к Регламенту (для юридических лиц), выдана соответствующая доверенность на совершение действий, определенных положениями настоящего Регламента для Пользователя УЦ.

В Таблице 1 приводятся рекомендуемые сроки действия сертификатов ключей проверки ЭП Пользователей УЦ, а также членов группы администраторов и сотрудников УЦ, обладающих правом доступа к функциям ПАК УЦ «Notary-PRO» в соответствии с принятым ролевым разграничением.

Таблица 1.

№ п/п	Владелец сертификата	Срок
1.	Удостоверяющий центр (при условии использования организационно-технического разделения ключа на несколько частей или неизвлекаемых ключей ЭП)	3 года
2.	Оператор Регистрационного центра	1 год

3.	Пользователь УЦ	1 год

5.3. Меры защиты ключей ЭП

Ключи электронной подписи Пользователей УЦ должны изготавливаться с использованием средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным в соответствии с №63-ФЗ «Об ЭП».

Ключи ЭП при их генерации должны записываться на отчуждаемые носители ключевой информации.

Ключи ЭП, изготовленные и записанные на ключевой носитель сотрудником УЦ, передаются Заявителю (Владельцу) лично или курьерской связью, в защищенном сейф-пакете.

Удостоверяющий центр не осуществляет депонирование и/или архивирование ключей электронных подписей Заявителей.

В качестве носителей ключевой информации допускается использование только тех устройств, которые указаны в формуляре средства электронной подписи, использовавшегося при их генерации.

Ключи ЭП на отчуждаемом носителе рекомендуется защищать паролем. Пароль формирует лицо, выполняющее процедуру генерации ключей, учитывая следующие требования:

- длина пароля должна быть не менее 6 символов;
- пароль должен содержать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

Если процедуру генерации ключей Пользователя УЦ выполняет сотрудник Удостоверяющего центра, то он должен сообщить сформированный пароль Владельцу ключа ЭП.

Ответственность за конфиденциальность пароля возлагается на Владельца ключа ЭП.

Требования данного раздела распространяются и на создаваемые резервные копии ключей ЭП.

Запрещается выполнять резервное копирование ключевых носителей с экспортируемыми ключами ЭП стандартными средствами операционной системы. Резервное копирование должно выполняться только с использованием сертифицированного СКЗИ.

Сотрудники Удостоверяющего центра, являющиеся Владельцами ключей ЭП, также должны выполнять требования данного раздела настоящего Регламента.

5.4. Копия сертификата ключа проверки ЭП в электронной форме

Копия сертификата ключа проверки ЭП Пользователя УЦ в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую рекомендации Международного союза телекоммуникаций ITU-T X.509 версии 3 и стандарту IETF (Internet Engineering Task Force) RFC 5280, и представленный в кодировке Base64.

5.5. Копия сертификата ключа проверки ЭП на бумажном носителе

Копия сертификата ключа проверки ЭП Пользователя УЦ на бумажном носителе представляет собой документ, содержащий следующие обязательные реквизиты:

- серийный номер сертификата ключа проверки ЭП;
- идентификационные данные Владельца сертификата;
- идентификационные данные издателя сертификата (идентификационные данные из сертификата ключа проверки ЭП Удостоверяющего центра);
- сведения о ключе проверки ЭП Владельца сертификата и алгоритме его формирования;
- сведения об областях использования ключа ЭП и сертификата;
- собственноручную подпись руководителя Удостоверяющего центра;
- печать Удостоверяющего центра.

Копия сертификата ключа проверки ЭП печатается в 2 экземплярах на листах белой бумаги формата А4, не содержащих средств защиты от копирования и подделки. Первый экземпляр – экземпляр Владельца сертификата, второй экземпляр – экземпляр Удостоверяющего центра.

5.6. Архивное хранение документированной информации

5.6.1. Состав архивных документов

Архивированию подлежит следующая документированная информация:

- реестр сертификатов ключей проверки ЭП Пользователей УЦ;
- сертификаты ключей проверки ЭП Удостоверяющего центра;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего центра (если таковые существуют);
- реестр зарегистрированных Пользователей УЦ;
- заявления на изготовление ключей Пользователей УЦ;
- заявления на изготовление сертификатов ключей проверки ЭП Пользователей УЦ;
- заявления на аннулирование (отзыв) сертификатов ключей проверки ЭП;
- служебные документы Удостоверяющего центра.

5.6.2. Комплектование архивного фонда

Решение вопросов комплектования архивного фонда Удостоверяющего центра возлагается на руководство Удостоверяющего центра.

5.6.3. Архивное хранилище

Архивные документы хранятся в специально оборудованном помещении – архивном хранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

5.6.4. Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов устанавливается в соответствии со сроками, определенными Федеральным законодательством.

5.6.5. Хранение сертификатов ключей подписей в Удостоверяющем центре

Срок хранения сертификата ЭП в Удостоверяющем центре осуществляется в течение всего периода его действия и 5 (Пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты ЭП переводятся в режим архивного хранения.

5.6.6. Уничтожение архивных документов

Решение вопросов уничтожения архивных документов Удостоверяющего центра возлагается на руководство Удостоверяющего центра.

6. Структуры сертификатов и списка отозванных сертификатов

6.1. Структура сертификатов ключей проверки ЭП, формируемых Удостоверяющим центром

Удостоверяющий центр формирует сертификаты ключей проверки ЭП Пользователей УЦ в электронной форме формата X.509 версии 3.

6.1.1. Базовые поля сертификата ключа проверки ЭП

Сертификаты ключей проверки ЭП содержат следующие базовые поля X.509:

Поле	Описание
Version	версия сертификата формата X.509
SerialNumber	уникальный серийный (регистрационный) номер сертификата в реестре сертификатов ключей проверки ЭП Удостоверяющего центра
Signature	идентификатор алгоритма подписи
Issuer	идентифицирующие данные УЦ
Validity	даты начала и окончания срока действия сертификата
Subject	идентифицирующие данные Владельца сертификата ключа проверки ЭП
SubjectPublicKeyInformation	идентификатор алгоритма и значение ключа проверки ЭП
extensions	расширения сертификата ключа проверки ЭП

6.1.2. Расширения сертификата ключа проверки ЭП

Сертификаты ключей проверки ЭП могут содержать следующие расширения:

Расширение	Описание
AuthorityKeyIdentifier	идентификатор ключа издателя сертификата
SubjectKeyIdentifier	идентификатор ключа Владельца сертификата

KeyUsage	назначение ключа
CertificatePolicies	сертификационные политики
SubjectAlternativeName	альтернативное имя Владельца
IssuerAlternativeName	альтернативное имя издателя
BasicConstraints	основные ограничения
ExtendedKeyUsage	расширенное назначение ключа
CRL DistributionPoints	адрес Списка отозванных сертификатов

6.1.3. Объектные идентификаторы алгоритмов

Удостоверяющий центр «Notary-PRO» использует идентификаторы алгоритмов средств электронной (цифровой) подписи в соттветствии с «Идентификаторы объектов (OID) Технического комитета по стандартизации «Криптографическая защита информации»».

6.1.4. Формы имени

В сертификате ключа проверки ЭП поля идентификационных данных Удостоверяющего центра и Владельца сертификата содержат атрибуты имени формата X.500.

6.1.5. Атрибуты имени

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, являются:

Атрибут	Описание
CountryName (C)	страна (код России в Стандарте ISO 3166 — RU)
CommonName (CN)	полное имя (фамилия, имя, отчество)
Surname (SN)	фамилия
givenName (GN)	имя и отчество (если имеется)
E-mail	адрес электронной почты

Обязательными атрибутами поля идентификационных данных Владельца сертификата, являющегося физическим лицом, представляющим юридическое лицо, являются:

Атрибут	Описание
CountryName(C)	страна (код России в Стандарте ISO 3166 — RU)
StateOrProvinceName	субъект Российской Федерации, где зарегистрирована организация,

(SP)	которую представляет Владелец сертификата
LocalityName (L)	город, где зарегистрирована организация, которую представляет Владелец сертификата
OrganizationName (O)	наименование организации, которую представляет Владелец сертификата
OrganizationalUnitName (OU)	наименование подразделения организации, которую представляет Владелец сертификата
CommonName (CN)	полное имя или краткое наименование организации, которую представляет Владелец сертификата
Surname (SN)	фамилия
givenName (GN)	имя и отчество (если имеется)
E-mail	адрес электронной почты

Обязательными атрибутами поля идентификационных данных уполномоченного лица Удостоверяющего центра являются:

Атрибут	Описание
CountryName (C)	страна (код России в Стандарте ISO 3166 — RU)
StateOrProvinceName (SP)	субъект Российской Федерации, где зарегистрирована организация, которую представляет Владелец сертификата
LocalityName (L)	город, где зарегистрирована организация, которую представляет Владелец сертификата
OrganizationName (O)	наименование организации, являющейся Владельцем УЦ
CommonName (CN)	наименование удостоверяющего центра
E-mail	адрес электронной почты уполномоченного лица УЦ

6.2. Структура СОС, формируемого Удостоверяющим Центром

Удостоверяющий центр издает Списки аннулированных (отозванных) сертификатов ключей проверки ЭП в электронной форме формата X.509 версии 2.

6.2.1. Базовые поля СОС

Списки аннулированных (отозванных) сертификатов содержат следующие расширения:

Название	Описание

Version	версия СОС формата X.509
Signature Algorithm	идентификатор алгоритма подписи
Issuer	издатель СОС
thisUpdate	время издания СОС
nextUpdate	время, по которое действителен СОС
revokedCertificates	список аннулированных (отозванных) и приостановленных сертификатов
crlExtensions	расширения СОС

6.2.2. Расширения СОС

Список аннулированных (отозванных) сертификатов может содержать следующие расширения:

Расширение	Описание
Authority Key Identifier	идентификатор ключа издателя списка аннулированных (отозванных) и приостановленных сертификатов

6.2.3. Расширения записей списка аннулированных (отозванных) сертификатов

Записи списка аннулированных (отозванных) сертификатов могут содержать следующие расширения:

Расширение	Описание
CRL Reason	причина отзыва сертификата

В качестве причины отзыва сертификата могут использоваться следующие значения:

Код	Идентификатор	Причина отзыва	Описание
0	Unspecified	Не указана	Отзыв сертификата без указания причины отзыва. Не рекомендуется для использования.
1	KeyCompromise	Компрометация ключа	Компрометация ключа ЭП владельца сертификата (утеря, раскрытие, искажение ключа, утеря ключа с последующим обнаружением, факт или подозрение того, что ключ стал известен другим лицам, нарушение правил хранения ключа ЭП).
2	CACompromise	Компрометация ключа УЦ	Компрометация ключа ЭП УЦ. При отзыве сертификата УЦ могут быть отозваны все сертификаты, выпущенные с его помощью.

3	AffiliationChanged	Смена владельца	Изменение сведений, указанных в сертификате (увольнение с работы, перевод на другую должность, смена персональных данных владельца сертификата, выявление ошибок в реквизитах).
4	Superseded	Смена ключа	Физическая порча ключевого носителя, невозможность воспроизведения пароля к ключу.
5	CessationOfOperation	Прекращение работы УЦ	Прекращение деятельности УЦ. Устанавливает запрет для сертификата УЦ на выпуск новых сертификатов пользователей, разрешая только выпуск Списков отозванных сертификатов.
6	CertificateHold	Приостановление действия	Приостановление действия сертификата при подозрении на компрометацию ключа ЭП (до выяснения обстоятельств). Приостановленный сертификат позднее может быть восстановлен или отозван с указанием другой причины.
9	PrivilegeWithdrawn	Ограничение привилегий	Изменение должностных обязанностей владельца сертификата или обстоятельств, на основании которых было предоставлено право подписи.

7. Рекомендации по обеспечению безопасности информации при эксплуатации СКЗИ

7.1. Ключи ЭП Владельцев сертификатов при их генерации должны записываться на отчуждаемые носители ключевой информации.

7.2. В качестве носителей ключевой информации допускается использование только тех устройств, которые указаны в формуляре средства электронной подписи, использовавшегося при их генерации.

7.3. Ключи ЭП пользователя относятся к конфиденциальной информации. Пользователь должен обеспечить надежное хранение в тайне своего ключа ЭП.

7.4. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

7.5. При хранении ключей необходимо обеспечить невозможность доступа к ключевым носителям лиц, не назначенных для работы с конкретным ключевым носителем.

7.6. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации.

7.7. Ключи ЭП на отчуждаемом носителе рекомендуется защищать паролем. Пароль формирует лицо, выполняющее процедуру генерации ключей, учитывая следующие требования:

- длина пароля должна быть не менее 6 символов;
- пароль должен содержать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

7.8. Если процедуру генерации ключей ЭП выполняет сотрудник Удостоверяющего центра, то он должен сообщить сформированный пароль Владельцу ключа ЭП.

7.9. Ответственность за конфиденциальность пароля возлагается на Владельца ключа ЭП.

7.10. Запрещается выполнять резервное копирование ключевых носителей стандартными средствами операционной системы. Резервное копирование должно выполняться только с использованием сертифицированного СКЗИ.

Приложение 1
Для юридических лиц

Заявление о присоединении к регламенту удостоверяющего центра

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____, в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра, условия которого определены УЦ «e-Notary» и опубликованы на сайте Удостоверяющего центра по адресу https://www.e-notary.ru/info/reglament.

С Регламентом Удостоверяющего центра и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

Руководитель организации _____ /_____ /

(подпись) (расшифровка подписи)

М.П.

_____

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо

Удостоверяющего центра _____ /_____ /

(подпись) (расшифровка подписи)

М.П.

Приложение 1
Для физических лиц и
индивидуальных предпринимателей

Заявление о присоединении к регламенту удостоверяющего центра

Я, _____

(фамилия, имя, отчество)

_____

(серия и номер паспорта)

_____,

(кем и когда выдан)

в соответствии со статьей 428 ГК Российской Федерации полностью и безусловно присоединяется к Регламенту Удостоверяющего центра, условия которого определены УЦ «e-Notary» и опубликованы на сайте Удостоверяющего центра по адресу https://www.e-notary.ru/info/reglament.

С Регламентом Удостоверяющего центра и приложениями к нему ознакомлен и обязуюсь соблюдать все положения указанного документа.

_____ /_____/

(подпись заявителя) (расшифровка подписи)

_____

(заполняется уполномоченным лицом Удостоверяющего центра)

Данное Заявление о присоединении к Регламенту Удостоверяющего зарегистрировано в реестре Удостоверяющего центра.

Регистрационный № _____ от «_____» _____ 20___ г.

Уполномоченное лицо

Удостоверяющего центра _____ /_____/

(подпись) (расшифровка подписи)

М.П.

Приложение 2
Для юридических лиц

ДОВЕРЕННОСТЬ №

г. Москва _____

(число, месяц и год выдачи доверенности прописью)

_____, доверяет

(полное наименование организации, включая организационно правовую форму)

_____

(ф.и.о. полностью, должность)

паспорт серии _____ № _____ выдан _____
_____ «____» _____ _____ г.

совершать от имени _____

(наименование организации)

действия в рамках Регламента Удостоверяющего центра «e-Notary», установленные для Пользователя Удостоверяющего центра.

В целях выполнения данного поручения он уполномочен подписывать и получать от имени организации-доверителя все документы, связанные с его выполнением.

Подпись удостоверяем _____ /_____

(Ф.И.О. удостоверяемого) (подпись удостоверяемого)

Доверенность действительна по «____» _____ 20__ г.

Руководитель организации _____ /_____ /

(подпись) (расшифровка подписи)

Главный бухгалтер _____ /_____ /

(подпись) (расшифровка подписи)

М.П.

Приложение 3
Для юридических лиц

Главному Администратору
Удостоверяющего центра «e-Notary»
Карпову И.О.

Заявление
на регистрацию Пользователя в Удостоверяющем центре, формирование ключей электронной подписи и изготовление сертификата ключа проверки электронной подписи

_____
(полное наименование организации, включая организационно-правовую форму)
в лице _____,
(должность)
_____
(фамилия, имя, отчество)
действующего на основании Устава, просит зарегистрировать уполномоченного представителя, _____
(ф.и.о. полностью, должность)
паспорт серии _____ _____ выдан _____
_____ ,
в реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленными Регламентом Удостоверяющего центра, сформировать ключи электронной подписи и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	
Surname (SN)	
givenName (GN)	
E-Mail (E)	
OrganizationName (O)	
OrganizationalUnitName (OU)	
Title (T)	
LocalityName (L)	
StateOrProvinceName (SP)	
CountryName (C)	
INN	
OGRN	
SNILS	

Настоящим заявлением _____
(фамилия, имя, отчество)
соглашается с обработкой своих персональных данных Удостоверяющим центром и признает, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого он является, относятся к общедоступным персональным данным.

Уполномоченный представитель _____ / _____ /
(подпись) (расшифровка подписи)
Руководитель организации _____ / _____ /
(подпись) (расшифровка подписи)

М.П.

«___» _____20__г.

Приложение 3
Для физических лиц

Главному Администратору

Удостоверяющего центра «e-Notary»

Карпову И.О.

Заявление

на регистрацию Пользователя в Удостоверяющем центре, формирование ключей электронной подписи и изготовление сертификата ключа проверки электронной подписи

Я,_____,

паспорт _____ _____, выдан _____,

прошу зарегистрировать меня в реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленными Регламентом Удостоверяющего центра, сформировать ключи электронной подписи и изготовить сертификат ключа проверки электронной подписи в соответствии с указанными в настоящем заявлении идентификационными данными:

CommonName (CN)	
Surname (SN)	
givenName (GN)	
E-Mail (E)	
LocalityName (L)	
StateOrProvinceName (SP)	
CountryName (C)	RU
SNILS	
INN	

Настоящим заявлением я, _____,

соглашаюсь с обработкой своих персональных данных Удостоверяющим центром и признаю, что персональные данные, заносимые в сертификат ключа проверки электронной подписи, владельцем которого я являюсь, относятся к общедоступным персональным данным.

_____ /_____ /

(подпись) (расшифровка подписи)

«___» _____ 20__ г.

Приложение 4
Для юридических лиц

Заявление на изготовление сертификата ключа проверки электронной подписи

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

в лице
_____
_____,
(должность)

_____
_____,
(фамилия, имя, отчество)

действующего на основании _____,

просит изготовить сертификат ключа проверки электронной подписи уполномоченного представителя_____
_____,
(фамилия, имя, отчество уполномоченного представителя)

в соответствии с указанными в настоящем заявлении данными и копией запроса на сертификат:

CommonName (CN)	
Surname (SN)	
givenName (GN)	
E-mail	
Title (T)	
OrganizationName (O)	
OrganizationalUnitName (OU)	
LocalityName (L)	
StateOrProvinceName (SP)	
CountryName(C)	
INN	
OGRN	
SNILS	

Настоящим заявлением_____
(фамилия, имя, отчество уполномоченного представителя)

соглашается с обработкой своих персональных данных АО «СИГНАЛ-КОМ» и признает, что персональные данные, заносимые Удостоверяющим центром «e-Notary» в сертификаты ключей подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Уполномоченный представитель_____/_____/
(подпись) (расшифровка подписи)

Руководитель организации_____/_____/
(подпись) (расшифровка подписи)

М.П.

«___» _____ 20__ г.

Приложение 4
Для физических лиц

Заявление на изготовление сертификата ключа проверки электронной подписи

Я, _____
(фамилия, имя, отчество)

паспорт _____ _____ _____
(серия и номер паспорта, кем и когда выдан)

_____

прошу изготовить сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с указанными в настоящем заявлении данными и копией запроса на сертификат:

CommonName (CN)	
Surname (SN)	
givenName (GN)	
E-mail	
LocalityName (L)	
StateOrProvinceName (SP)	
CountryName(C)	
INN	
SNILS	

Настоящим заявлением я соглашаюсь с обработкой своих персональных данных АО «СИГНАЛ-КОМ» и признаю, что персональные данные, заносимые Удостоверяющим центром «e-Notary» в сертификаты ключей подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

_____/_____/
(подпись) (расшифровка подписи)

«___» _____ 20__ г.

Приложение 5
Для юридических лиц

КАРТОЧКА РЕГИСТРАЦИИ ЗАПРОСА НА СЕРТИФИКАТ АБОНЕНТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА "e-Notary"

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

в лице _____,

_____,
(фамилия, имя, отчество)

действующего на основании _____, просит зарегистрировать уполномоченного представителя,

_____,
(фамилия, имя, отчество)

паспорт серии _____ № _____ выдан _____ «____» _____ _____ г., в реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленными Регламентом Удостоверяющего центра, и изготовить сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с полным текстом запроса на сертификат:

——BEGIN CERTIFICATE REQUEST——

——END CERTIFICATE REQUEST——

Настоящим заявлением _____
(фамилия, имя, отчество уполномоченного представителя)

соглашается с обработкой своих персональных данных АО «СИГНАЛ-КОМ» и признает, что персональные данные, заносимые Удостоверяющим центром «e-Notary» в сертификаты ключей проверки электронных подписей, владельцем которых он является, относятся к общедоступным персональным данным.

Уполномоченный представитель _____/_____/
(подпись) (расшифровка подписи)

Руководитель организации _____/_____/
(подпись) (расшифровка подписи)

М.П.

«_____» _____ 20___ г.

Приложение 5
Для физических лиц

КАРТОЧКА РЕГИСТРАЦИИ ЗАПРОСА НА СЕРТИФИКАТ АБОНЕНТА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА "e-Notary"

Я, _____
(фамилия, имя, отчество)

_____
(серия и номер паспорта)

_____,
(кем и когда выдан)

прошу зарегистрировать меня в реестре Удостоверяющего центра, наделить полномочиями Пользователя Удостоверяющего центра, установленными Регламентом Удостоверяющего центра, и изготовить сертификат ключа проверки электронной подписи уполномоченного представителя в соответствии с полным текстом запроса на сертификат:

——BEGIN CERTIFICATE REQUEST——

——END CERTIFICATE REQUEST——

Настоящим заявлением я, _____,
(фамилия, имя, отчество)

соглашаюсь с обработкой своих персональных данных АО «СИГНАЛ-КОМ» и признаю, что персональные данные, заносимые Удостоверяющим центром «e-Notary» в сертификаты ключей проверки электронных подписей, владельцем которых я являюсь, относятся к общедоступным персональным данным.

_____/_____/
(подпись заявителя) (расшифровка подписи)

М.П.

«_____» _____ 20___ г.

Приложение 6

Форма заявления на отзыв сертификата

Администратору УЦ «e-Notary»

(для юридических лиц оформляется на бланке организации)

Заявление на отзыв сертификата

Прошу Вас отозвать сертификат, идентифицируемый перечисленными ниже параметрами:

(Серийный номер сертификата)	(Аварийный пароль)

изготовленный для _____

(фамилия, имя, отчество Владельца сертификата)

в соответствии с_____

(номер Договора на изготовление и обслуживание сертификатов)

Данный сертификат прошу изъять из обращения и занести его в список отозванных сертификатов в связи с

_____

Владелец сертификата / Руководитель организации

_____ / _____ /

(подпись) (расшифровка)

М.П.

«_____» _____ 20__ г.

Приложение 7

Форма заявления на отзыв доверенности

Администратору УЦ e-Notary

(для юридических лиц оформляется на бланке организации)

Заявление на отзыв доверенности

_____

(полное наименование организации, включая организационно-правовую форму)

в лице _____,

(должность)

_____,

(фамилия, имя, отчество)

действующего на основании _____, заявляет, что Доверенность № ____ от «____» _____ _____ года, выданную своему уполномоченного представителю – Пользователю Удостоверяющего центра: _____

(ф.и.о. полностью, должность)

паспорт серии _____ № _____ выдан _____ «____» _____ _____ г., позволяющую от имени _____

(наименование организации)

осуществлять действия в рамках Регламента Удостоверяющего центра и просит аннулировать (отозвать) все действующие сертификаты ключей проверки электронных подписей, владельцем которых является_____.

(фамилия, имя, отчество)

Руководитель организации _____ /_____ /

(подпись) (расшифровка подписи)

Главный бухгалтер _____ /_____ /

(подпись) (расшифровка подписи)

М.П.

«_____» _____ 20___ г.

Приложение 8

Руководство
по порядку использования и обеспечению безопасности использования электронных подписей и средств электронной подписи

Термины и определения

Владелец сертификата ключа проверки электронной подписи (владелец сертификата) - лицо, которому в установленном Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи - уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка ЭП).

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации.

Компрометация ключа электронной подписи - утрата доверия к тому, что используемые ключи электронной подписи недоступны посторонним лицам или подозрение, что ключи электронной подписи были временно доступны неуполномоченным лицам. К событиям, связанным с компрометацией ключа электронной подписи, относятся (включая, но не ограничиваясь):

- физическая утрата ключевого носителя;
- потеря ключевого носителя с его последующим обнаружением;
- передача ключа электронной подписи по открытым каналам связи;
- перехват ключа электронной подписи вредоносным программным обеспечением;
- несанкционированный доступ постороннего лица к устройству хранения ключа электронной подписи;
- случаи, когда невозможно достоверно установить, что произошло с ключевым носителем, в том числе случаи выхода ключевого носителя из строя;
- сознательная передача ключа электронной подписи постороннему лицу;
- увольнение сотрудников, имевших доступ к ключу электронной подписи юридического лица;
- нарушение правил хранения ключевой информации.

Конфиденциальная информация - сведения, независимо от формы их предоставления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством РФ.

Несанкционированный доступ к информации - доступ к информации в нарушение должностных полномочий сотрудника или доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации.

Сертификат ключа проверки электронной подписи (сертификат) - электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Средства электронной подписи (далее - средства ЭП) - шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Удостоверяющий центр - юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

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.

1. Риски, связанные с использованием электронной подписи.

К основным рискам, связанным с использованием электронной подписи, относятся:

1.1. Несанкционированное подписание электронного документа электронной подписью, которое может быть произведено в результате:

- компрометации ключа электронной подписи;
- подмены подписываемого документа в результате работы на компьютере вредоносного программного обеспечения.

1.2. Негативные последствия, вызванные невозможностью подписания электронного документа электронной подписью, обусловленной следующими событиями:

- уничтожение (удаление с ключевого носителя) ключа и/или сертификата ключа проверки электронной подписи;
- неисправность ключевого носителя, на котором хранятся ключ и/или сертификата ключа проверки электронной подписи;
- блокировка ключевого носителя, вызванная неоднократным вводом некорректного кода доступа (пароля или ПИН-кода);
- физическая утрата ключевого носителя.

1.3. Риск фальсификации электронной подписи.

Данный риск является скорее гипотетическим, но при использовании несертифицированного средства ЭП или использовании средства ЭП, полученного нелегально, в том числе и не определенным для данного средства способом, может породить следующие реальные риски:

- Риски отказа автора от своей электронной подписи под электронным документом или признания электронной подписи под электронным документом недействительной, которые могут быть аргументированы возможностью подделки электронной подписи при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. не обладающих гарантированной криптографической стойкостью).

- Риск отказа автора от содержания подписанного электронной подписью электронного документа, которое может быть аргументировано возможностью модификации подписываемого документа при использовании несертифицированных или полученных нелегальным путем средств ЭП (т.е. обладающего недекларированными возможностями).

В целях снижения рисков, связанных с использованием электронной подписи, необходимо выполнение комплекс организационно-технических и административных мер по обеспечению безопасности использования электронной подписи и средств электронной подписи.

2. Порядок получения сертифицированных средств ЭП.

Способы получения средств ЭП:

- при личном посещении офиса УЦ;
- через доставку курьером, службами экспресс-доставки, заказными бандеролями и др. в опечатанном и пронумерованном сейф-пакете; сейф-пакет опечатывается таким образом, что любая попытка его вскрытия не может остаться незамеченной;
- путем загрузки дистрибутива ПО со страницы Портала УЦ, по каналу, защищенному протоколом TLS с использованием стандартных средств браузера, с обязательным последующим выполнением процедуры контроля целостности ПО с помощью сертифицированной ФСБ России утилиты для вычисления хэш и эталонной контрольной суммы, которые необходимо получить по другим каналам.

3. Организация работ по обеспечению безопасности использования электронной подписи и средств электронной подписи.

3.1. Безопасность использования электронной подписи и средств ЭП должна обеспечиваться на всех этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.
3.2. Правом доступа к рабочим местам с установленными средствами ЭП должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Каждый пользователь, применяющий средства ЭП, должен быть ознакомлен с настоящим Руководством и документацией на средства ЭП.

4. Требования по размещению технических средств с установленными средствами ЭП.

При размещении технических средств с установленными на них средствами ЭП:

4.1. Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным средствами ЭП, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.
4.2. Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ, сохранность доверенных им конфиденциальных документов и сведений, включая ключи электронной подписи.

5. Требования по установке средств ЭП, а также общесистемного и специального программного обеспечения.

5.1. Установку общесистемного и специального программного обеспечения (далее - ПО), а также средств ЭП, должны осуществлять лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и средство ЭП.
5.2. При установке средств ЭП следует:

- На технических средствах, предназначенных для работы со средствами ЭП, использовать только лицензионное программное обеспечение фирм - изготовителей.
- На компьютере не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода средств ЭП и приложений, использующих средства ЭП, а также для просмотра кода и областей памяти, используемой средствами ЭП, в процессе обработки средствами ЭП информации и/или при загруженной ключевой информации.
- Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены средства ЭП (например, путем опечатывания системного блока и разъемов компьютера).
- Программное обеспечение, устанавливаемое на компьютер с установленным средством ЭП, не должно содержать возможностей, позволяющих:
    - модифицировать содержимое произвольных областей памяти;
    - модифицировать собственный код и код других программ;
    - модифицировать память, выделенную для других программ;
    - передавать управление в область собственных данных и данных других программ;
    - несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
    - модифицировать настройки операционной системы (далее - ОС);
    - использовать недокументированные фирмой-разработчиком функции ОС.

6. Требования по защите от несанкционированного доступа при эксплуатации средств ЭП.

При организации работ по защите информации от несанкционированного доступа (далее - НСД) необходимо руководствоваться требованиями эксплуатационной документации на соответствующее средство ЭП, а также учитывать следующие общие требования:

6.1. Необходимо использовать пароли, сформированные в соответствии со следующими правилами:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 года.

6.2. Запрещается:

- оставлять без контроля компьютер или мобильное устройство, на котором эксплуатируются средства ЭП, после ввода ключевой информации либо иной конфиденциальной информации;

- вносить какие-либо изменения в программное обеспечение средств ЭП;
- осуществлять несанкционированное копирование ключевых носителей;

• разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
• использовать ключевые носители в режимах, не предусмотренных функционированием средств ЭП.

6.3. Должна быть исключена установка на компьютере или мобильном устройстве программ, позволяющих, пользуясь особенностями ОС, повышать предоставленные привилегии.
6.4. Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
6.5. При подключении компьютера с установленными средствами ЭП к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.
6.6. При использовании средств ЭП на компьютерах, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют средства ЭП, и к компонентам средств ЭП со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.
6.7. Необходимо использовать средства антивирусной защиты.
6.8. Необходимо исключить одновременную работу средств ЭП различных производителей.
6.9. К работе со средствами допускаются лица, изучившие настоящее Руководство и пользовательскую документацию на средства ЭП.

7. Требования по защите от несанкционированного доступа к ключевой информации при использовании специализированных ключевых носителей (аппаратных токенов).

7.1. После получения аппаратного токена (типа JaCarta, Рутокен и пр.) пользователь должен произвести смену предустановленных на нем PIN-кодов пользователя и администратора, используемых для аутентификации. Значения предустановленных PIN-кодов указаны в эксплуатационной документации на соответствующий аппаратный токен.
7.2. PIN-коды должны состоять не менее чем из 6 символов. Символы могут включать в себя как буквы и цифры, так и знаки препинания и т. п., т. е. любые символы, которые можно ввести со стандартной клавиатуры.
7.3. При эксплуатации аппаратного токена необходимо учитывать, что после введения неправильного PIN-кода пользователя несколько раз подряд токен блокируется. Разблокировать токен можно при помощи PIN-кода администратора В случае введения несколько раз подряд неправильного PIN администратора разблокировка токена становится невозможной.
7.4. В ходе эксплуатации аппаратного токена рекомендуется производить смену действующих PIN- кодов с периодичностью, не превышающей 6 месяцев.

8. Действии при компрометации ключей электронной подписи.

8.1. Пользователь самостоятельно должен определить факт компрометации ключа электронной подписи, оценить значение этого события и выполнить мероприятия по розыску и локализации последствий компрометации ключа электронной подписи.
8.2. При компрометации ключа электронной подписи пользователь должен немедленно сообщить в Удостоверяющий центр о факте компрометации. Информация о компрометации должна передаваться в Удостоверяющий центр способом, определенным Регламентом

Удостоверяющего центра. По получении информации о компрометации ключа электронной подписи Удостоверяющий центр прекращает действие сертификата соответствующего ключа проверки электронной подписи, в результате чего создание действительной электронной подписи с использованием скомпрометированного ключа электронной подписи становится невозможным.