

**НАЦИОНАЛЬНЫЙ
УДОСТОВЕРЯЮЩИЙ ЦЕНТР**

«УТВЕРЖДАЮ»
Генеральный директор



Щербина И.Е.

Щербина И.Е.

10 января 2008 г

РЕГЛАМЕНТ

услуг Удостоверяющего центра



СОДЕРЖАНИЕ

1	Основы деятельности национального удостоверяющего центра	- 5 -
1.1	Сведения об Удостоверяющем центре	- 5 -
1.2	Структура Удостоверяющего центра	- 5 -
1.3	Адреса размещения Центров регистрации:	- 6 -
1.4	Публикация сведений об Удостоверяющем центре.....	- 7 -
1.5	Точки распространения списка отозванных сертификатов (CRL)	- 7 -
2	Порядок работы Удостоверяющего центра	- 7 -
2.1	Введение	- 7 -
2.1.1	Используемые сокращения	- 7 -
2.1.2	Основные понятия и определения	- 7 -
2.2	Общие положения.....	- 12 -
2.2.1	Статус Регламента.....	- 12 -
2.2.2	Толкование Регламента.....	- 12 -
2.2.3	Изменения (дополнения) Регламента.....	- 13 -
2.2.4	Назначение Удостоверяющего центра	- 13 -
2.2.5	Перечень услуг, предоставляемых Удостоверяющим центром	- 14 -
2.2.6	Клиенты Удостоверяющего центра	- 15 -
2.2.7	Пользователь сертификата	- 16 -
2.2.8	Участники споров. Разрешение споров	- 16 -
2.2.9	Оплата услуг.....	- 16 -
2.2.10	Присоединение к Регламенту	- 16 -
2.2.11	Расторжение договорных отношений (выход из Регламента)	- 17 -
2.2.12	Прекращение деятельности Удостоверяющего центра	- 18 -
2.3	Политика конфиденциальности	- 18 -
2.3.1	Конфиденциальная информация.....	- 18 -
2.3.2	Неконфиденциальная информация	- 18 -
2.3.3	Исключительные полномочия официальных лиц.....	- 19 -
2.4	Используемые криптографические алгоритмы	- 19 -
2.5	Регистрация Клиентов.....	- 20 -
2.5.1	Процедура регистрации нового Клиента	- 20 -

2.5.2	Перечень документов, предоставляемых в Удостоверяющий центр при заключении договора о присоединении к Регламенту между Удостоверяющим центром и Клиентом	- 20 -
2.6	Выпуск сертификата.....	- 22 -
2.6.1	Процедура выпуска сертификата.....	- 22 -
2.6.2	Перечень документов, предоставляемых для получения сертификата	- 22 -
2.6.3	Выпуск сертификата для вычислительного устройства или программного приложения -	23 -
2.7	Изготовление электронных ключей (ключевой пары) в Центре регистрации	- 23 -
2.7.1	Требования к АРМ, используемым для генерации электронных ключей (ключевой пары)-	23 -
2.7.2	Изготовление электронных ключей (ключевой пары)	- 24 -
2.8	Управление сертификатами Клиентов и электронными ключами.....	- 24 -
2.9	Приостановление действия сертификата	- 25 -
2.9.1	Приостановление действия сертификата по заявлению в электронной форме.....	- 25 -
2.9.2	Приостановление действия сертификата по заявлению в письменной форме.....	- 26 -
2.9.3	Приостановление действия сертификата по заявлению в устной форме.....	- 26 -
2.9.4	Требования к содержанию и оформлению письменного Заявления о приостановление действия сертификата.....	- 27 -
2.10	Возобновление действия сертификата	- 28 -
2.10.1	Возобновление действия сертификата по заявлению в электронной форме.....	- 28 -
2.10.2	Возобновление действия сертификата по заявлению в письменной форме.....	- 29 -
2.10.3	Требования к содержанию и оформлению письменного Заявления о возобновлении действия сертификата.....	- 29 -
2.11	Аннулирование (отзыв) сертификата	- 30 -
2.11.1	Отзыв сертификата по инициативе владельца сертификата	- 30 -
2.11.2	Отзыв сертификата по инициативе собственника сертификата (юридического лица)	- 31 -
2.12	Плановая смена ключей Уполномоченного лица Удостоверяющего центра.....	- 31 -
2.13	Подтверждение подлинности ЭЦП.....	- 32 -
2.13.1	Процедура подтверждения ЭЦП в ЭД с использованием сертификата	- 33 -
2.13.2	Процедура подтверждения ЭЦП Уполномоченного лица Удостоверяющего центра в сертификате	- 35 -
2.13.3	Документ, подтверждающий факт обладания электронными ключами, зарегистрированными в Удостоверяющем центре	- 36 -
2.14	Представление информации о компрометации секретного (закрытого) ключа	- 37 -

2.14.1	Компрометация закрытого (секретного) ключа владельца сертификата.....	- 37 -
2.14.2	Компрометации электронных ключей Удостоверяющего центра	- 38 -
2.15	Порядок согласования нового Регламента с Клиентом.....	- 38 -
2.16	Сертификат	- 40 -
2.16.1	Базовые поля сертификата.....	- 40 -
2.16.2	Дополнения сертификата	- 40 -
2.16.3	Объектные идентификаторы алгоритма	- 41 -
2.16.4	Формы имени (атрибуты имени).....	- 41 -
2.16.5	Ограничения на имена.....	- 41 -
2.17	Сроки действия сертификатов	- 42 -
2.17.1	Сроки действия ключей Уполномоченного лица Удостоверяющего центра.....	- 42 -
2.18	Сроки хранения сертификатов в реестре	- 43 -
2.19	Список отозванных сертификатов	- 43 -
2.19.1	Основные базовые поля в СОС (CRL).....	- 43 -
2.19.2	Дополнения СОС (CRL)	- 44 -
2.20	Архивное хранение документированной информации	- 44 -
2.20.1	Состав архивируемых документов.....	- 44 -
2.20.2	Источник комплектования архивного фонда.....	- 45 -
2.20.3	Архивохранилище.....	- 45 -
2.20.4	Срок архивного хранения	- 45 -
2.20.5	Уничтожение архивных документов.....	- 45 -
2.21	Список приложений	- 45 -
	Приложение №1 к Регламенту.....	- 47 -
	Приложение №2 к Регламенту.....	- 48 -
	Приложение №3 к Регламенту.....	- 50 -
	Приложение №4 к Регламенту.....	- 51 -
	Приложение №5 к Регламенту.....	- 52 -
	Приложение №6 к Регламенту.....	- 53 -
	Приложение №7 к Регламенту.....	- 54 -
	Приложение №8 к Регламенту.....	- 57 -
	Приложение №9 к Регламенту.....	- 58 -
	Приложение №10 к Регламенту.....	- 59 -

1 ОСНОВЫ ДЕЯТЕЛЬНОСТИ НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

1.1 Сведения об Удостоверяющем центре

Некоммерческое партнерство «Национальный удостоверяющий центр», именуемое в дальнейшем «Удостоверяющий центр», зарегистрировано на территории Российской Федерации в городе Москва. Свидетельство о регистрации № 002.011.898, выдано 28.08.2000г. Московской регистрационной палатой.

Удостоверяющий центр в качестве участника рынка по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей осуществляет свою деятельность на территории Российской Федерации.

Юридический адрес: 127018, г. Москва, ул.Образцова, д.38.

Почтовый адрес: 117630, г.Москва, Старокалужское шоссе 58, стр.1, к.1424

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

ИНН/КПП 7715246020/771501001

Счет № 40703810700060000024

в ОАО Внешторгбанк в г.Москве,

к/с 30101810700000000187,

БИК 044525187

Контактные телефоны, факс, адрес электронной почты:

тел./факс: (495) 330-80-33 / 333-52-98; Web: <http://www.nucrf.ru>; e-mail: nuc@nucrf.ru

1.2 Структура Удостоверяющего центра

Национальный удостоверяющий центр включает в свой состав следующие организационные подразделения (службы):

1. Служба администрирования Удостоверяющего центра, выполняет следующие функциональные задачи:

- управление деятельностью Удостоверяющего центра;

- координация деятельности служб Удостоверяющего центра;
- взаимодействие с Клиентом (пользователями услуг) в части разрешения вопросов, связанных с применением средств ЭЦП, электронных ключей (ключевой пары) и сертификатов, изготавливаемых и/или распространяемых Удостоверяющим Центром;
- взаимодействие с Клиентами (пользователями услуг) в части разрешения вопросов, связанных с подтверждением ЭЦП Уполномоченного лица Удостоверяющего центра в сертификатах, выпущенных Национальным Удостоверяющим Центром в электронной форме, подтверждением собственноручной подписи уполномоченного лица Удостоверяющего центра в копиях сертификатов, изготовленных на бумажном носителе.

2. Служба регистрации клиентов – Центр регистрации, выполняет следующие функциональные задачи:

- подготовка договоров между Клиентом и Удостоверяющим центром;
- регистрация Клиентов в качестве пользователей услуг Удостоверяющего центра;
- ведение реестра зарегистрированных пользователей Удостоверяющего центра;
- предоставление вновь зарегистрированному Клиенту электронных ключей (ключевой пары);
- формирование запроса на выпуск сертификата;
- распространение средств электронной цифровой подписи и шифрования.

3. Служба безопасности Удостоверяющего центра, выполняет следующие функциональные задачи:

- организация и выполнение мероприятий по защите ресурсов Удостоверяющего центра;
- контроль деятельности служб Удостоверяющего центра;
- изготовлению электронных ключей (ключевой пары) по обращению пользователей УЦ;
- архивное хранение сертификатов.

1.3 Адреса размещения Центров регистрации:

Московский Центр регистрации: 117630, г. Москва, Старокалужское шоссе, д.58, стр.1.
Тел./факс: 8(495) 330-80-33, 8(495) 333-52-98.

Адреса других центров регистрации, а также Удаленных центров регистрации публикуются на сайте Удостоверяющего центра по URL адресу: <http://www.nucrf.ru>

1.4 Публикация сведений об Удостоверяющем центре

Сертификат Удостоверяющего центра опубликован по URL адресу: <http://nucrf.ru/download/ta.cer>. Наименование сертификата Удостоверяющего центра в URL адресе может меняться в зависимости от версии действующего сертификата.

Дополнительные сведения об Удостоверяющем центре и его деятельности можно прочитать на сайте Удостоверяющего центра по URL адресу: <http://www.nucrf.ru>

1.5 Точки распространения списка отозванных сертификатов (CRL)

Список отозванных сертификатов пользователей услуг Удостоверяющего центра опубликован по URL адресу: <http://nucrf.ru/download/ta.crl>. Наименование файла списка отзыва сертификатов в URL адресе может меняться в зависимости от версии действующего списка отзыва сертификатов.

2 ПОРЯДОК РАБОТЫ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

2.1 Введение

2.1.1 Используемые сокращения

АС – автоматизированная система

АРМ – автоматизированное рабочее место.

ЭЦП – электронная цифровая подпись

ЭД – электронный документ

СОС – список отозванных сертификатов (CRL – Certificate Revocation List)

2.1.2 Основные понятия и определения

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Целостность информации - состояние защищенности информации, характеризуемое способностью АС обеспечивать сохранность и неизменность конфиденциальной

информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения.

Пользователь (потребитель) информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Закрытый (секретный) ключ – последовательность символов, известная владельцу сертификата и не подлежащая разглашению. Закрытый ключ используется для формирования электронной цифровой подписи и/или расшифрования данных.

Открытый ключ – последовательность символов, свободно распространяемая в виде открытой информации всем участникам информационного взаимодействия (физическим лицам), связанная с закрытым (секретным) ключом с помощью особого математического соотношения. Открытый ключ используется для проверки электронной цифровой подписи в электронных документах и их зашифрования, при этом, открытый ключ не позволяет вычислить значение закрытого (секретного) ключа.

Ключевая пара (электронные ключи) – открытый и закрытый ключи, связанные между собой особым математическим соотношением.

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого (секретного) ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Электронная цифровая подпись – это строка бит, полученная в результате процесса формирования подписи и имеющая внутреннюю структуру, которая зависит от конкретного механизма формирования подписи.

Ключевой контейнер – представляет собой специальным образом организованный электронный каталог, содержащий файлы с ключевым материалом: закрытый (секретный) ключ, сертификат. Ключевой контейнер записывается на ключевой носитель. Для предотвращения возможности несанкционированного использования закрытого (секретного) ключа посторонними лицами, ключевой контейнер защищают паролем. Ключевой контейнер может содержать не более одного ключа подписи и не более одного ключа шифрования. Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности.

Ключевой носитель – внешнее (съемное) устройство, используемое для хранения ключевых контейнеров с закрытыми (секретными) ключами. Один ключевой носитель может содержать один или несколько ключевых контейнеров с различными ключами.

Компрометация закрытого ключа – результат действий физического лица, повлекший за собой разглашение закрытого (секретного) ключа.

Криптопровайдер (Cryptographic Service Provider - провайдер услуг шифрования) – библиотека функций, в которой реализованы непосредственно криптографические алгоритмы или через которую осуществляется доступ к аппаратному шифратору.

Сертификат ключа подписи – документ на бумажном носителе либо электронный документ, включающий в свою структуру открытый ключ формирования электронной цифровой подписи, помогающий другим пользователям установить, является ли закрытый (секретный) ключ, применяемый для формирования ЭЦП, подлинным (достоверным). Сертификат ключа подписи используется для предотвращения возможных попыток выдачи ключевой пары одного человека за ключевую пару другого человека. Электронный сертификат заверяется электронной цифровой подписью Уполномоченного лица Удостоверяющего центра.

Сертификат ключа шифрования – документ на бумажном носителе либо электронный документ, включающий в свою структуру открытый ключ шифрования и информацию о его владельце. Сертификат ключа шифрования создается Удостоверяющим центром для выполнения криптографических преобразований открытой информации электронного документа (шифрование/расшифрование электронного документа). Электронный сертификат шифрования заверяется электронной цифровой подписью Уполномоченного лица Удостоверяющего центра.

Сертификат (сертификат открытого ключа) – общее название сертификатов ключа подписи/шифрования, это электронный документ либо его аналог на бумажном носителе, в структуру которого внесена информация об открытом ключе и его владельце. Электронный сертификат заверяется электронной цифровой подписью Уполномоченного лица Удостоверяющего центра.

Список отозванных сертификатов (CRL) - электронный документ с электронной цифровой подписью Уполномоченного лица Удостоверяющего центра, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны,

либо действие которых было приостановлено. Сертификаты, чьи номера присутствуют в списке файла CRL, являются отозванными из обращения Удостоверяющим центром.

Владелец сертификата – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат, владеющее закрытым (секретным) ключом, соответствующим открытому ключу, включенному в состав сертификата, выданного на его имя.

Собственник сертификата – юридическое или физическое лицо, связанное договорными отношениями с Удостоверяющим центром, являющееся инициатором выпуска сертификата на имя владельца сертификата и совершившее оплату услуг по выпуску данного сертификата.

Средство криптографической защиты информации (СКЗИ) – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Удостоверяющий центр – (центр по удостоверению подлинности сертификатов) юридическое лицо или выделенное подразделение юридического лица, обладающие полномочиями на удостоверение принадлежности конкретного открытого ключа, включенного в структуру электронного сертификата, определенному физическому лицу владельцу сертификата.

Доверенный источник времени – источник доверенного времени (юридическое либо физическое лицо), предоставляющее по запросу любого владельца сертификата метку времени, подписанную собственной электронной цифровой подписью, которую в свою очередь запросивший метку времени владелец сертификата включает в структуру собственной электронной цифровой подписи при подписи электронного документа. Источнику доверенного времени доверяют все пользователи информационного взаимодействия.

Клиент – юридическое или физическое лицо, пользующееся услугами другого физического или юридического лица, вступающее с ним в деловые отношения, оформленные письменным договором.

Оператор Удостоверяющего центра – физическое лицо, являющееся работником Удостоверяющего центра, занимающееся рассмотрением и обработкой заявлений на изготовление, аннулирование (отзыв), приостановление/возобновление действия сертификатов ключей подписи.

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся работником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов и Списков отозванных сертификатов.

Рассмотрение заявления на аннулирование (отзыв), приостановление/возобновление действия сертификата ключа подписи – принятие решения уполномоченным работником Удостоверяющего центра об осуществлении обработки заявления на основании представленных Клиентом документов в Удостоверяющий центр.

Рабочий день Удостоверяющего Центра (далее – рабочий день) – промежуток времени с 9 часов 30 минут до 18 часов каждого дня недели за исключением субботы, воскресенья и праздничных нерабочих дней.

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

- реестр заключенных договоров о присоединении к Регламенту Удостоверяющего центра;
- реестр заключенных договоров об оказании услуг Удостоверяющим центром;
- реестр поступивших заявлений об изготовлении сертификата;
- реестр поступивших заявлений об аннулировании (отзыве) сертификата;
- реестр поступивших заявлений о приостановлении/возобновлении действия сертификата;
- реестр изготовленных сертификатов;
- реестр изготовленных Списков отозванных сертификатов.

Электронный документ - форма подготовки, отправления, получения или хранения информации с помощью электронных технических средств, зафиксированная на магнитном диске, магнитной ленте, лазерном диске и ином электронном материальном носителе.

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:

- PKCS#7 (RFC 2315) – стандарт, определяющий формат и синтаксис криптографических сообщений; Удостоверяющий Центр использует описанный в PKCS#7 тип данных PKCS#7 Signed – подписанные данные;

– PKCS#10 (RFC2986) – стандарт, определяющий формат и синтаксис запроса на сертификат ключа подписи.

2.2 Общие положения

2.2.1 Статус Регламента

В соответствии с законодательством Российской Федерации разработан «Регламент услуг Удостоверяющего центра», именуемый в дальнейшем «Регламент».

Настоящий Регламент описывает общий порядок и условия предоставления услуг Удостоверяющим центром для своих Клиентов (владельцев сертификата), присоединившихся к Регламенту в порядке, предусмотренном статьёй 428 «Договор о присоединении к Регламенту», ГК РФ либо заключивших «Договор на оказание услуг».

Настоящий Регламент является неотъемлемой частью договора о присоединении к Регламенту и является основополагающим документом, на основании которого формируются права и обязанности заинтересованных сторон, детально изложенных договоре о присоединении к Регламенту.

Любое заинтересованное лицо может ознакомиться с содержанием Регламента и договора о присоединении к Регламенту, обратившись к ресурсу сайта Удостоверяющего центра по адресу <http://www.nucrf.ru>, либо в любом из выше перечисленных офисов Удостоверяющего центра.

Основанием для начала предоставления услуг Клиенту Удостоверяющий центр считает факт подписания договора о присоединении к Регламенту и/или договора об оказании услуг, заключаемых между Клиентом и Удостоверяющим центром, и совершение оплаты услуг в соответствии заключенному договору.

2.2.2 Толкование Регламента

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

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

2.2.3 Изменения (дополнения) Регламента

Внесение изменений (дополнений) в Регламент, в том числе в приложения к нему, производится Удостоверяющим центром в одностороннем порядке.

Уведомление Клиентов и пользователей информации о внесении изменений/дополнений в Регламент осуществляется Удостоверяющим центром путем размещения указанных изменений (дополнений) на сайте Удостоверяющего центра по URL адресу: <http://www.nucrf.ru>.

Все изменения (дополнения), вносимые Удостоверяющим центром в настоящий Регламент по собственной инициативе и не связанные с изменением законодательства РФ, могут быть связаны с улучшением условий предоставления действующих услуг, добавления нового вида услуг, изменением адресов регистрации и размещения Центров регистрации, а также адресов размещения электронных ресурсов, изменениями в структуре Удостоверяющего центра, и вступают в силу и становятся обязательными для участников договорных отношений по истечении 30 (тридцати) календарных дней с даты опубликования нового Регламента на сайте Удостоверяющего центра.

Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех Клиентов Удостоверяющего центра, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений/дополнений в силу.

Все изменения/дополнения, вносимые Удостоверяющим центром в Регламент в связи с изменением законодательства РФ, регулирующего деятельность Удостоверяющих центров, вступают в силу одновременно с вступлением в силу законодательных актов.

Идентификация Регламента осуществляется по дате его утверждения.

2.2.4 Назначение Удостоверяющего центра

Национальный Удостоверяющий Центр предназначен для обеспечения участников корпоративных информационных систем средствами и спецификациями для использования сертификатов открытых ключей в целях обеспечения:

- применения электронной цифровой подписи;
- контроля целостности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем;
- аутентификации участников информационных систем в процессе взаимодействия;

– конфиденциальности информации, представленной в электронном виде, передаваемой в процессе взаимодействия участников информационных систем.

2.2.5 Перечень услуг, предоставляемых Удостоверяющим центром

Удостоверяющий центр предоставляет Клиентам следующие виды услуг:

- внесение в реестр Удостоверяющего центра регистрационной информации о Клиенте;
- формирование ключевой пары (закрытый и открытый ключи) с последующей их записью на ключевой носитель, по запросу Клиента;
- изготовление сертификатов для Клиента в электронной форме;
- изготовление копии сертификатов для владельца сертификата на бумажном носителе;
- ведение реестра изготовленных Удостоверяющим центром сертификатов;
- предоставление сертификатов в электронной форме из реестра изготовленных сертификатов, по запросам пользователей информации;
- аннулирование (отзыв) сертификатов открытых ключей по обращениям владельцев сертификатов/собственников сертификатов;
- приостановление и возобновление действия сертификатов открытых ключей по обращениям владельцев сертификатов;
- предоставление пользователям информации сведений об аннулированных (отозванных) сертификатах и сертификатах с приостановленным сроком действия;
- подтверждение подлинности электронных цифровых подписей в документах, представленных в электронной форме, по обращению Клиента;
- подтверждение подлинности электронной цифровой подписи уполномоченного лица Удостоверяющего центра в изготовленных им сертификатах открытых ключей по запросу Клиента;
- распространение средств электронной цифровой подписи.

2.2.6 Клиенты Удостоверяющего центра

Удостоверяющий центр предоставляет свои услуги физическим и юридическим лицам. Юридическое лицо может пользоваться услугами Удостоверяющего центра через своего представителя – физическое лицо, на которое оформлены соответствующие документы, подтверждающие его право представлять интересы юридического лица.

Удостоверяющий центр, в качестве своего Клиента, регистрирует физическое лицо, так как сертификат может быть выпущен только на имя физического лица (владельцем сертификата может являться только физическое лицо).

Собственником сертификата может быть как физическое лицо, так и юридическое лицо. Права собственности на сертификат для физического или юридического лица определяются в зависимости от того, кто из вышеназванных субъектов является инициатором заключения договорных отношений с Удостоверяющим центром и оплачивает в рамках заключенного договора услуги Удостоверяющего центра (является основным плательщиком).

Клиенты Удостоверяющего центра разделяются на три группы:

Группа 1 – физические лица, зарегистрированные в Удостоверяющем центре и обладающие «временным» сертификатом – сертификат является служебным, имеет ограниченный срок действия (2 недели), предназначен для входа в электронную систему Центра регистрации Удостоверяющего центра через открытую сеть Интернет с удаленного АРМ Клиента с целью формирования запроса на выпуск рабочего сертификата; при формировании запроса на выпуск «рабочего» сертификата Клиент самостоятельно генерирует электронные ключи (ключевую пару);

Группа 2 – физические лица, зарегистрированные в Удостоверяющем центре и обладающие «рабочим» сертификатом;

Группа 3 – физические и юридические лица, не зарегистрированные в Удостоверяющем центре, но обращающиеся к его услугам для получения открытой информации о владельцах сертификатов

Группа 4 – физические и юридические лица, не зарегистрированные в Удостоверяющем центре, но заключившие договор на оказание услуг для проверки статуса и подлинности сертификатов, подписанных Уполномоченным лицом Удостоверяющего центра, а также проверки подлинности ЭЦП, сформированных Клиентами группы 2.

2.2.7 Пользователь сертификата

Пользователем сертификата может быть любое физическое лицо, устройство или программное приложение.

2.2.8 Участники споров. Разрешение споров

В случае возникновения споров в части оказания услуг Удостоверяющим центром участниками спора (сторонами спора) считаются Удостоверяющий центр и собственник сертификата (физическое или юридическое лицо).

В случае возникновения споров между владельцами сертификатов, являющимися участниками информационного взаимодействия и Клиентами Удостоверяющего центра, сторонами спора считаются собственники сертификата (физические или юридические лица). В данном случае Удостоверяющий центр может быть привлечен для разрешения спорных вопросов в качестве независимого эксперта.

2.2.9 Оплата услуг

Удостоверяющий центр осуществляет свою деятельность на платной основе.

Перечень услуг Удостоверяющего центра, стоимость и порядок их оплаты определяются в индивидуальном порядке на основании договора о присоединении к Регламенту (Договора об оказании услуг) заключенного между заинтересованными сторонами.

В случае, если инициатором внеплановой смены (перевыпуска) действующих сертификатов Клиентов выступает Удостоверяющий центр, смена (перевыпуск) действующих сертификатов и сертификатов с приостановленным сроком действия осуществляется Удостоверяющим центром без взимания дополнительной оплаты со своих Клиентов (безвозмездно) с сохранением статуса сертификата, действующего на момент выполнения операции по их замене.

2.2.10 Присоединение к Регламенту

Чтобы стать Клиентом Удостоверяющего центра физическому или юридическому лицу необходимо заключить с Удостоверяющим центром «Договор о присоединении к Регламенту» либо «Договор об оказании услуг», произвести своевременную оплату услуг в соответствии заключенному договору и предоставить необходимый перечень документов

для осуществления регистрации нового Клиента (см. раздел 2.5) или выполнения проверки и подтверждения подлинности ЭЦП по запросу (см. раздел 2.13).

2.2.11 Расторжение договорных отношений (выход из Регламента)

Клиент имеет право в одностороннем порядке, без обращения в суд, расторгнуть действующий договор о присоединении к Регламенту.

Для расторжения действующего договора с Удостоверяющим центром Клиенту достаточно:

1) если Клиент – юридическое лицо, являющееся собственником сертификатов физических лиц, необходимо предоставить в Центр регистрации Удостоверяющего центра письменное уведомление установленной формы (приложение №3 к настоящему Регламенту) о намерении расторгнуть действующие договорные отношения с Удостоверяющим центром; Удостоверяющий центр на основании представленного документа отзывает все действующие сертификаты физических лиц, представляющих интересы юридического лица, выпущенные по расторгаемому договору (сертификаты, имеющие статус приостановленного действия также отзываются); датой расторжения договора считается дата, последующего 2 (второго) дня за датой опубликования списка отозванных сертификатов;

2) если Клиент – физическое лицо, являющееся собственником сертификатов:

– необходимо отозвать все действующие сертификаты, выпущенные Удостоверяющим центром; по истечении 1 месяца со дня отзыва всех действующих сертификатов и отсутствия в названный срок письменного обращения со стороны Клиента о выпуске нового сертификата договор с клиентом считается расторгнутым;

– либо, необходимо направить через открытую сеть Интернет электронное уведомление установленной формы (приложение №3 к настоящему Регламенту), подписанное личной ЭЦП (ЭЦП формируется при помощи действующего сертификата, выпущенного Удостоверяющим центром); Удостоверяющий центр на основании представленного электронного документа аннулирует все действующие сертификаты Клиента и возвращает по электронной почте, через открытую сеть Интернет, электронное уведомление Клиента, подписанное ЭЦП уполномоченного лица Удостоверяющего центра, датой расторжения договора считается дата штампа времени источника доверенного времени, присутствующая в ЭЦП уполномоченного лица Удостоверяющего центра.

2.2.12 Прекращение деятельности Удостоверяющего центра

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

В случае прекращения деятельности Удостоверяющего центра реестр Удостоверяющего центра, включающий в свой состав реестр зарегистрированных Клиентов – владельцев сертификатов и реестр изготовленных сертификатов, передается в Корневой Удостоверяющий центр либо в Удостоверяющий центр, наделенный соответствующими полномочиями со стороны Корневого Удостоверяющего центра (г. Москва). Передача сведений осуществляется по согласованию между всеми заинтересованными сторонами.

2.3 Политика конфиденциальности

2.3.1 Конфиденциальная информация

Удостоверяющий центр выделяет следующие типы конфиденциальной информации и порядок обращения с ней:

- секретный (закрытый) ключ владельца сертификата, Удостоверяющий центр не депонирует и не архивирует секретные (закрытые) ключи Клиентов;
- пароль доступа к контейнеру с секретным (закрытым) ключом, сформированному по запросу Клиента, сообщается только его будущему владельцу, физическому лицу на чье имя выпущен соответствующий секретному (закрытому) ключу сертификат;
- персональная и корпоративная информация Клиентов (пользователей услуг) не подлежащая внесению в содержание электронного сертификата и в состав списка отозванных сертификатов, не подлежит разглашению;
- информация, хранящаяся в журналах аудита Удостоверяющего центра, не подлежит разглашению;
- отчетные материалы по выполненным проверкам деятельности Удостоверяющего центра, не подлежат разглашению;

2.3.2 Неконфиденциальная информация

Удостоверяющий центр выделяет следующие типы информации общего доступа:

- информация, включаемая в сертификаты открытых ключей владельцев сертификатов;

- информация, включаемая в списки отозванных сертификатов;
- законодательно-нормативные документы, регламентирующие работу Удостоверяющих центров;

- копии сертификатов от организаций, имеющих право выдавать лицензии, на программные продукты СКЗИ, программно аппаратные комплексы «Удостоверяющий центр», на осуществление деятельности Удостоверяющего центра в области оказания услуг;

- заключения о результатах проверок деятельности Удостоверяющего центра;
- информация о настоящем Регламенте.

Информация общего доступа публикуется по решению Удостоверяющего центра. Место, способ и время публикации информации общего доступа определяется самостоятельным решением Удостоверяющего центра и выполняются в соответствии настоящему Регламенту.

2.3.3 Исключительные полномочия официальных лиц

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

2.4 Используемые криптографические алгоритмы

Программное обеспечение АРМ пользователей услуг Удостоверяющего центра должно обеспечивать возможность использования следующих алгоритмов СКЗИ:

- ГОСТ 34.10-2001 (уникальный идентификационный номер – “1.2.643.2.2.19”);
- ГОСТ 34.11-94 (уникальный идентификационный номер – “1.2.643.2.2.9”);
- ГОСТ 28147-89 (уникальный идентификационный номер – “1.2.643.2.2.21”).

Пользователь обязан соблюдать условия эксплуатации СКЗИ строго в соответствии с инструкциями разработчика СКЗИ и требованиями руководящих документов органов исполнительной власти, осуществляющих контроль в области разработки, распространения и эксплуатации СКЗИ.

Пользователь обязан хранить в тайне закрытый ключ ЭЦП и принимать необходимые меры для предотвращения его компрометации.

2.5 Регистрация Клиентов

Процедура регистрации Клиента (пользователя услуг) применяется в отношении физического или юридического лица, заключивших договор о присоединении к Регламенту с Удостоверяющим центром.

2.5.1 Процедура регистрации нового Клиента

Регистрация нового Клиента осуществляется в соответствии следующему алгоритму действий:

- оформление Договора о присоединении к Регламенту между Клиентом и Удостоверяющим центром;
- оплата услуг в соответствии действующему договору;
- оформление и регистрация документов, представленных Клиентом для проведения процедуры его регистрации (см. раздел 2.5.2);
- регистрация Клиента в реестре Центра регистрации в качестве пользователя услуг Удостоверяющего центра;
- для вновь зарегистрированного Клиента (пользователя услуг) осуществляется выпуск электронного сертификата и его дубликата на бумажном носителе. По заявлению Клиента предварительно перед выпуском сертификата могут быть сформированы электронные ключи.

2.5.2 Перечень документов, предоставляемых в Удостоверяющий центр при заключении договора о присоединении к Регламенту между Удостоверяющим центром и Клиентом

Лицо (заявитель), желающее пройти процедуру регистрации в Удостоверяющем центре, должно заключить Договор о присоединении к Регламенту с Удостоверяющим центром. Дополнительно в Центр регистрации Удостоверяющего центра заявитель должен предоставить следующий перечень документов:

1) Если заявитель – физическое лицо, представляет личные интересы и предполагает в будущем использовать персональную ЭЦП, при обмене информацией с участниками информационного взаимодействия, для обозначения своих личных интересов, то он должен представить следующие документы:

- личный паспорт, и ксерокопию второй и третьей страниц паспорта;
- адрес электронной почты;

- контактные телефоны;
- данные для удаленной идентификации владельца сертификата (ключевая фраза длиной до 64 символов);

2) Если заявитель - физическое лицо, выступает в роли представителя интересов юридического лица и предполагает в будущем использовать персональную ЭЦП, при обмене информацией с участниками информационного взаимодействия, для обозначения интересов юридического лица, то он должен представить следующие документы:

- список работников для выпуска сертификатов (приложение № 9 к настоящему Регламенту), подписанный уполномоченным представителем юридического лица, в котором прописаны его фамилия, имя и отчество, должность, занимаемая в организации и адрес электронной почты;

- письменное согласие физического лица (будущего владельца сертификата) с тем, что на его имя будет выпущен сертификат (приложение №8 к настоящему Регламенту);

- личный паспорт, и ксерокопию второй и третьей страниц паспорта;

- заверенный юридическим лицом документ, подтверждающий правомочность уполномоченного представителя юридического лица действовать от имени этого юридического лица;

- нотариально заверенную копию документа, подтверждающего государственную регистрацию организации, чьи интересы представляет физическое лицо.

В случае, если от имени юридического лица действует физическое лицо, наделенное полномочиями представлять интересы как самой организации (юридического лица), так и интересы физических лиц, на имя которых организация намерена приобрести сертификаты, то дополнительно к вышеназванному перечню потребуется представить:

- доверенность на изготовление электронных ключей (ключевой пары) от имени будущих владельцев сертификата (приложение № 1 или Приложение № 10 к настоящему Регламенту).

Примечание. Если будущий владелец сертификата ключа подписи намерен использовать выпущенный на его имя сертификат в приложениях, требующих дополнительные документы в качестве основания для выпуска сертификата, то такие документы также должны быть представлены при заключении договора о присоединении к Регламенту.

2.6 Выпуск сертификата

2.6.1 Процедура выпуска сертификата

Выпуск сертификата для Клиента осуществляется в соответствии следующему алгоритму действий:

- Клиент при посредничестве Центра регистрации заключает договор с Удостоверяющим центром о присоединении к Регламенту;
- Клиент на основании заключенного договора осуществляет оплату услуг Удостоверяющего центра;
- Клиент оформляет заявление о выпуске сертификата на основании заключенного договора;
- Центр регистрации на основании заявления Клиента и заключенного договора с помощью специализированного программного обеспечения формирует электронный запрос в Удостоверяющий центр;
- На основании электронного запроса предоставленного Центром регистрации в Удостоверяющий центр, Удостоверяющим центром выпускается электронный сертификат и изготавливает его дубликат на бумажном носителе. Электронный сертификат публикуется через Интернет-сайт Удостоверяющего центра, а его дубликат передается владельцу сертификата через Центр регистрации, участвующий в описанной цепочке событий.
- Клиент получает на руки электронный сертификат и устанавливает его на своем АРМ;
- Клиент обращается в Центр регистрации за заверенным дубликатом сертификата созданной на бумажном носителе.

2.6.2 Перечень документов, предоставляемых для получения сертификата

Для получения сертификата Клиенту необходимо предоставить в Центр регистрации копию и оригинал финансового документа, подтверждающего произведение платежа в рамках заключенного договора между Удостоверяющим центром и Клиентом и бланк запроса на выпуск сертификата открытого ключа (приложение № 9).

2.6.3 Выпуск сертификата для вычислительного устройства или программного приложения

В случаях, когда Клиент нуждается в сертификате, который ему необходим для настройки автоматизированной работы каких-либо электронно-вычислительных машин, устройств или программных приложений, ему необходимо:

– если Клиент – физическое лицо, запросить на свое имя новый сертификат с характеристиками, удовлетворяющими потребности электронно-вычислительных машин, устройств или программных приложений;

– если Клиент – юридическое лицо, назначить ответственное лицо, на имя которого будет выпущен сертификат, и вместе с запросом нового сертификата представить в Удостоверяющий центр документ, в котором отображены сведения о физическом лице, на имя которого требуется выпустить сертификат.

Процедуры регистрации уполномоченного лица Клиента и выпуска сертификата описаны в разделах 2.5, 2.6.

2.7 Изготовление электронных ключей (ключевой пары) в Центре регистрации

2.7.1 Требования к АРМ, используемым для генерации электронных ключей (ключевой пары)

Формирование электронных ключей (ключевой пары) должно осуществляться на специализированном АРМ Центра регистрации, а генерация электронных ключей должна выполняться аппаратным датчиком случайных чисел программно-аппаратного комплекса средств защиты от НСД, входящего в состав данного АРМ.

Для специализированных АРМ оператора (администратора) Центра регистрации, используемых для формирования электронных ключей (ключевой пары), предварительно, на этапе подготовки к работе, проводятся специальные исследования на побочные электромагнитные излучения и наводки (ПЭМИН) и специальные проверки на отсутствие электронных устройств негласного съема информации.

При эксплуатации специализированного АРМ должно соблюдаться требования технической и эксплуатационной документации применяемого СКЗИ по защите информации.

При генерации электронных ключей (ключевой пары) в Центре регистрации автоматически формируется, подписанный ЭЦП уполномоченного работника Центра регистрации, электронный запрос на выпуск сертификата в формате PKCS#10, который впоследствии направляется Удостоверяющий центр.

2.7.2 Изготовление электронных ключей (ключевой пары)

При обращении Клиента в Центр регистрации Удостоверяющего центра с просьбой о формировании электронных ключей (ключевой пары), процедуру формирования электронных ключей выполняют специально уполномоченные на проведение данной операции работники Центра регистрации. В процессе генерации секретный (закрытый) ключ автоматически размещается на ключевом носителе. В качестве ключевого носителя используются специализированные отчуждаемые устройства типа USB-брелок либо смарт-карта, позволяющие обеспечить сохранность и конфиденциальность записываемой на них информации. Клиент может получить на руки электронные ключи, записанные на ключевой носитель только в том Центре регистрации, в который он подавал запрос на выполнение данной процедуры. Факт передачи ключевого носителя из рук в руки документируется.

Удостоверяющий центр предоставляет своим Клиентам право самостоятельно формировать электронные ключи (ключевую пару), в случае если Клиент использует для генерации электронных ключей сертифицированные средства криптографической защиты информации. То есть, Клиент может самостоятельно изготовить электронные ключи и предоставить их на ключевом носителе в Центр регистрации для формирования запроса на изготовление сертификата в Удостоверяющий центр. Обязательным условием при подобном варианте взаимодействия с Клиентом является соответствие электронного формата представляемых электронных ключей (ключевой пары) формату электронных ключей, с которыми работает Удостоверяющий центр; в этом случае Удостоверяющий центр в лице Центра регистрации не несет ответственности перед Клиентом за сохранность электронных ключей (ключевой пары).

2.8 Управление сертификатами Клиентов и электронными ключами

Прямое управление сертификатами зарегистрированных пользователей осуществляет Удостоверяющий центр. Клиенты, владеющие сертификатами, могут управлять статусом личных сертификатов путем предоставления информации о своих намерениях в

Удостоверяющий центр либо в отделение Центра регистрации при посредничестве которого был заключен договор о присоединении к регламенту.

Информацию о всех происходящих изменениях с сертификатами Клиент может получить в специализированном разделе Интернет сайта Удостоверяющего центра. В данном разделе публикуется и регулярно обновляется следующая информация: списки отозванных сертификатов, действующие сертификаты Удостоверяющего центра. Предоставляются дополнительные инструменты поиска нужного сертификата в общем списке всех выпущенных сертификатов, а также выполнения проверки их статуса в режиме Online.

Клиент самостоятельно эксплуатирует электронные ключи (ключевую пару) без вмешательства Удостоверяющего центра.

2.9 Приостановление действия сертификата

Приостановление действия сертификата, осуществляется Удостоверяющим центром по заявлению Клиента, являющегося владельцем сертификата. Заявления о приостановлении действия сертификата принимаются Центрами регистрации в электронной, письменной и устной формах.

На основании принятого заявления Удостоверяющий центр отзывает сертификат на срок, указанный в заявлении, и публикует о нем сведения в списке отозванных сертификатов (CRL). Возобновить действие сертификата можно в любой момент времени периода действия срока его отзыва. Если в течение, указанного в заявлении, периода действия срока отзыва сертификата его владелец не обратился в Центр регистрации с просьбой об изменении статуса сертификата (предоставление заявления о возобновлении действия сертификата), сертификат считается аннулированным.

Датой и временем определяющими момент, с которого сертификат считается временно отозванным (имеет статус сертификата с приостановленным сроком действия), признаются следующие за принятием заявления от Клиента дата и время публикации списка отозванных сертификатов.

2.9.1 Приостановление действия сертификата по заявлению в электронной форме

Клиент может направить в адрес Удостоверяющего центра по электронной почте заявление о приостановлении действия сертификата в виде электронного документа,

подписанного личной ЭЦП. Заголовок электронного письма и название файла электронного документа должны соответствовать его содержанию. Обязательными условиями при приеме к рассмотрению данного вида заявления являются: использование Клиентом при формировании ЭЦП электронных ключей (ключевой пары) соответствующих действующему сертификату; подтверждение Клиентом своих намерений в результате телефонного звонка в Удостоверяющий центр.

Срок рассмотрения запроса о приостановлении действия сертификата в электронной форме составляет 3 (три) рабочих дня с момента поступления электронного письма по электронной почте.

2.9.2 Приостановление действия сертификата по заявлению в письменной форме

Клиент может подать письменное заявление о приостановлении действия личного сертификата собственноручно, при личном прибытии в Центр регистрации, либо через доверенное лицо, на имя которого оформлена письменная доверенность, заверенная нотариусом. Форма заявления о приостановлении действия сертификата приведена в приложении №4 к настоящему Регламенту.

При личном прибытии Клиента заявление о приостановлении действия сертификата принимается в любом Центре регистрации, адреса офисов указаны в разделе 1.3 настоящего Регламента.

При представлении заявления о приостановлении действия сертификата через доверенное лицо, прием заявления осуществляется только в том Центре регистрации, в котором был оформлен и подписан договор о присоединении к Регламенту между Клиентом и Удостоверяющим центром и была выполнена процедура регистрации Клиента в качестве нового пользователя услуг.

Срок рассмотрения заявления о приостановлении действия сертификата составляет 1 (один) рабочий день с момента приема заявления от владельца сертификата.

2.9.3 Приостановление действия сертификата по заявлению в устной форме

Удостоверяющий центр принимает от своих Клиентов заявления о приостановлении действия сертификата, заявленные в устной форме с использованием средств телефонной связи.

Прием устного заявления от владельца сертификата осуществляется в Центре регистрации, в котором был заключен Договор о присоединении к Регламенту между Клиентом и Удостоверяющим центром и произведена регистрация Клиента в качестве пользователя услуг.

Пред приемом заявления Клиент проходит процедуру удаленной аутентификации. В случае успешного ее прохождения, Клиент по запросу работника Центра регистрации должен сообщить следующие сведения:

- серийный номер сертификата, действие которого приостанавливается;
- срок, на который приостанавливается действие сертификата;
- причина приостановки действия сертификата.

На основании представленных сведений работник Центра регистрации формирует запрос о приостановлении действия сертификата.

Срок рассмотрения заявления о приостановлении действия сертификата составляет 1 (один) рабочий день с момента приема заявления от владельца сертификата.

В период действия срока, на который сертификат был приостановлен, Клиент должен представить в Центр регистрации письменное заявление о приостановлении действия личного сертификата (порядок представления письменного заявления смотри в разделе 2.9.2 настоящего Регламента).

2.9.4 Требования к содержанию и оформлению письменного Заявления о приостановление действия сертификата

Заявление о приостановлении действия сертификата должно быть выполнено в рукописной (разборчивым почерком) или печатной форме на бумажном носителе формата А4, заверенное собственноручной подписью заявителя (см. приложение №4 к настоящему Регламенту).

В содержание заявления должны быть включены следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого приостанавливается;
- срок, на который приостанавливается действие сертификата;
- причина приостановки действия сертификата;

- дата и подпись заявителя.

2.10 Возобновление действия сертификата

Возобновление действия сертификата, осуществляется Удостоверяющим центром по заявлению Клиента, являющегося владельцем сертификата. Заявления о возобновлении действия сертификата принимаются Центрами регистрации в электронной и письменной формах.

На основании принятого заявления Удостоверяющий центр меняет статус сертификата с «отозванный» на «действующий», и убирает сведения о текущем сертификате из регулярно публикуемого списка отозванных сертификатов (CRL). Возобновить действие сертификата можно в любой момент времени периода действия срока на который он был отозван (календарные даты и время в течение которых действие сертификата приостановлено). Если в течение периода действия срока отзыва сертификата, Клиент не представил в Центр регистрации заявление о возобновлении действия сертификата - сертификат считается аннулированным.

2.10.1 Возобновление действия сертификата по заявлению в электронной форме

В случае наличия на руках Клиента электронных ключей (ключевой пары) с действующим сертификатом Клиент может направить в адрес Удостоверяющего центра по электронной почте заявление о возобновлении действия своего другого сертификата с приостановленным сроком действия в виде электронного документа, подписанного личной ЭЦП. Заголовок электронного письма и название файла электронного документа должны соответствовать его содержанию. Обязательными условиями при приеме к рассмотрению данного вида заявления являются: использование Клиентом при формировании ЭЦП электронных ключей (ключевой пары) соответствующих действующему сертификату; подтверждение Клиентом своих намерений в результате телефонного звонка в Удостоверяющий центр.

Срок рассмотрения запроса о приостановлении действия сертификата в электронной форме составляет 3 (три) рабочих дня с момента поступления электронного письма по электронной почте.

2.10.2 Возобновление действия сертификата по заявлению в письменной форме

Клиент может подать письменное заявление о возобновлении действия личного сертификата собственноручно, при личном прибытии в Центр регистрации, либо через доверенное лицо, на имя которого оформлена письменная доверенность, заверенная нотариусом. Форма заявления о возобновлении действия сертификата приведена в приложении №5 к настоящему Регламенту.

При личном прибытии Клиента заявление о приостановлении действия сертификата принимается в любом Центре регистрации, адреса офисов указаны в разделе 1.3 настоящего Регламента.

При представлении заявления о возобновлении действия сертификата через доверенное лицо, прием заявления осуществляется только в том в Центре регистрации, в котором был заключен договор о присоединении к Регламенту между Клиентом и Удостоверяющим центром и была выполнена процедура регистрации Клиента в качестве нового пользователя услуг.

Срок рассмотрения заявления о возобновлении действия сертификата составляет 1 (один) рабочий день с момента приема заявления от владельца сертификата.

2.10.3 Требования к содержанию и оформлению письменного Заявления о возобновлении действия сертификата

Заявление о возобновлении действия сертификата должно быть выполнено в рукописной (разборчивым почерком) или печатной форме на бумажном носителе формата А4, заверенное собственноручной подписью заявителя (см. приложение №5 к настоящему Регламенту).

В содержание заявления должны быть включены следующие обязательные реквизиты:

- идентификационные данные заявителя;
- серийный номер сертификата, действие которого возобновляется;
- причина возобновления действия сертификата;
- дата и подпись заявителя.

2.11 Аннулирование (отзыв) сертификата

Удостоверяющий центр отзывает действующие сертификаты по инициативе Клиента, являющегося:

- владельцем сертификата и его собственником
- владельцем сертификата;
- собственником сертификата.

Основанием для отзыва сертификата является представление в Центр регистрации Удостоверяющего центра заявления об аннулировании (отзыве) действующего сертификата от Клиента, являющегося его собственником либо владельцем. Форма заявления на аннулирование (отзыв) сертификата приведена в Приложении № 3 к настоящему Регламенту.

Удостоверяющий центр оставляет за собой право самостоятельно принимать решение о необходимости отзыва сертификата Клиента в случае выявления событий, связанных с компрометацией закрытого (секретного) ключа Клиента, либо Уполномоченного лица Удостоверяющего центра, чья подпись присутствует в действующих сертификатах Клиента, а также в случае проведения плановой смены сертификата Уполномоченного лица Удостоверяющего центра.

Если причиной отзыва сертификата Клиента является компрометация закрытого (секретного) ключа Уполномоченного лица Удостоверяющего центра либо проведение плановой смены сертификата Уполномоченного лица Удостоверяющего центра, выпуск нового сертификата для Клиента осуществляется Удостоверяющим центром самостоятельно без взимания комиссионного вознаграждения. Порядок выпуска нового сертификата вместо заменяемого описан в разделе 2.12.

2.11.1 Отзыв сертификата по инициативе владельца сертификата

Для отзыва действующего сертификата его владельцу необходимо представить в офис Центра регистрации Удостоверяющего центра заявление об аннулировании (отзыве) личного сертификата. Данное условие является достаточным для выполнения требования Клиента.

Порядок представления заявления об аннулировании (отзыве) сертификата идентичен порядку представления заявления о приостановлении действия сертификата. При принятии решения об аннулировании (отзыва) сертификата Клиенту для отзыва действующего сертификата следует руководствоваться разделами 2.9.1, 2.9.2, 2.9.3 настоящего Регламента.

Срок рассмотрения заявления об аннулировании (отзыве) действующего сертификата составляет 1 (один) рабочий день с момента приема заявления от владельца сертификата.

2.11.2 Отзыв сертификата по инициативе собственника сертификата (юридического лица)

Отзыв действующего сертификата по инициативе собственника сертификата, (юридического лица), осуществляется на основании следующих документов:

- заявление от руководителя организации об аннулировании (отзыве) сертификатов физических лиц, представляющих интересы юридического лица;
- список физических лиц (работников организации), чьи сертификаты требуется аннулировать (отозвать).

Прием выше названных документов осуществляется в офисе Центра регистрации, через который был оформлен и заключен договор о присоединении к Регламенту между Клиентом и Удостоверяющим центром.

Порядок представления документов идентичен процедуре представления заявления о приостановлении действия сертификата. При принятии решения об аннулировании (отзыве) сертификата Клиенту для отзыва действующего сертификата следует руководствоваться разделом 2.9.2 настоящего Регламента.

Срок рассмотрения заявления об аннулировании (отзыве) действующего сертификата составляет 1 (один) рабочий день с момента приема заявления от собственника сертификата.

2.12 Плановая смена ключей Уполномоченного лица Удостоверяющего центра

Плановая смена электронных ключей (ключевой пары) и выпуск нового сертификата Уполномоченного лица Удостоверяющего центра выполняется не позднее, чем за 2 (два) месяца до окончания срока действия соответствующего сертификату закрытого (секретного) ключа.

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

- для Уполномоченного лица Удостоверяющего центра формируются новые электронные ключи (ключевая пара) и соответствующий им сертификат;

– для клиентов в замен действующих сертификатов, подписанных ЭЦП Уполномоченного лица Удостоверяющего центра с использованием старого сертификата, выпускаются новые сертификаты, подписанные новой ЭЦП Уполномоченного лица: комиссионное вознаграждение за выпуск нового сертификата для Клиента Удостоверяющим центром с Клиента не взимается;

– на сайте Удостоверяющего центра размещаются сведения, информирующие всех Клиентов Удостоверяющего центра о выпуске новых сертификатов и способе их получения;

– по истечении срока действия старого сертификата Уполномоченного лица Удостоверяющий центр отзывает все ранее действующие сертификаты, которые были подписаны ЭЦП Уполномоченного лица Удостоверяющего центра с использованием закрытого (секретного) ключа соответствующего его устаревшему сертификату.

Старый закрытый (секретный) ключ используется для формирования списков отозванных сертификатов в электронной форме, издаваемых Удостоверяющим центром в период действия старого закрытого ключа Уполномоченного лица Удостоверяющего центра.

2.13 Подтверждение подлинности ЭЦП

Удостоверяющий центр осуществляет экспертную проверку ЭЦП:

– ЭЦП в ЭД, сформированных владельцами сертификатов, выпущенных Удостоверяющим центром;

– ЭЦП Уполномоченного лица Удостоверяющего центра, которая использовалась для подписи сертификатов Клиентов, действующих либо срок действия которых уже истек.

Основанием для проведения экспертной проверки ЭЦП является письменное заявление Клиента-заявителя (см. разделы 2.13.1, 2.13.2) и оплата предоставляемой услуги. Порядок оплаты и стоимость услуги определены в действующих тарифах Удостоверяющего центра. Перечень предлагаемых услуг и их стоимость (тарифы) публикуются в приложении к договору о присоединении к Регламенту, либо к договору об оказании услуг, которые заключаются между Клиентом и Удостоверяющим центром.

Перед принятием заявления Удостоверяющий центр принимает во внимание следующее необходимое условие его дальнейшего рассмотрения – между Клиентом и Удостоверяющим центром должен быть заключен договор, который предусматривает предоставление данной услуги. В результате рассмотрения вопроса могут возникнуть следующие ситуации:

1) между Клиентом и Удостоверяющим центром заключен договор о присоединении к Регламенту; договор является действующим и в его спецификацию включена номенклатурная позиция, описывающая данный вид услуги, в этом случае Клиенту достаточно предоставить заявление о подтверждении ЭЦП Уполномоченного лица Удостоверяющего центра и копию подписанного договора с приложенной спецификацией;

2) между Клиентом и Удостоверяющим центром заключен договор о присоединении к Регламенту, но в его спецификацию не включена номенклатурная позиция, описывающая данный вид услуги, либо между Клиентом и Удостоверяющим центром отсутствуют договорные отношения, в этом случае Клиенту необходимо заключить «Договор об оказании услуг», произвести оплату услуги в рамках заключенного договора и предоставить заявление о подтверждении ЭЦП Уполномоченного лица Удостоверяющего центра.

Заключить «Договор об оказании услуг» и подать Заявление о подтверждении ЭЦП, можно в любом Центре регистрации, адреса которых перечислены в разделе 1.3 настоящего Регламента.

2.13.1 Процедура подтверждения ЭЦП в ЭД с использованием сертификата

Подтверждение ЭЦП в ЭД осуществляется Центрами регистрации по обращению Клиентов, на основании представленного в письменной форме заявления о подтверждении ЭЦП в ЭД.

В представленном заявлении должна быть указана информация о дате и времени формирования ЭЦП в ЭД.

Бремя доказывания достоверности даты и времени формирования ЭЦП в ЭД возлагается на заинтересованную сторону – хозяина ЭЦП.

Обязательным приложением к заявлению о подтверждении ЭЦП в ЭД является внешний носитель электронной информации (дискета 3'5"), на котором записаны:

- исходный (неподписанный) файл ЭД, к которому применялась ЭЦП;
- файл ЭД, подписанный ЭЦП, авторство которого оспаривается;
- файл сертификата Уполномоченного лица Удостоверяющего центра, являющегося издателем сертификата, соответствующего закрытому (секретному) ключу, с помощью которого была сформирована ЭЦП в ЭД;
- файл списка отозванных сертификатов, издателем которого является Удостоверяющий центр, использовавшийся для проверки ЭЦП в ЭД заявителем.

- дистрибутивы СКЗИ.

Срок рассмотрения заявления о подтверждении ЭЦП в ЭД составляет 5 (пять) рабочих дней с момента его представления в Центр регистрации.

По результатам проверки Клиент получает на руки протокол (Акт) проверки ЭЦП в котором содержатся:

- результат проверки ЭЦП сертифицированным средством;
- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке (экспертизе) содержит следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, занимаемая должность);
- вопросы, поставленные перед экспертом или комиссией экспертов;
- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с Федеральным законом.

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

В случае отказа в рассмотрении заявления Клиента работник Центра регистрации вносит в его заявление свою резолюцию, раскрывающую причину отказа в рассмотрении поступившей заявки, снимает копию заявления. В оригинале заявления и в его копии Клиент ставит свою подпись, подтверждающую факт ознакомления с содержащейся в нем резолюцией работника Центра регистрации.

2.13.2 Процедура подтверждения ЭЦП Уполномоченного лица Удостоверяющего центра в сертификате

Подтверждение ЭЦП Уполномоченного лица Удостоверяющего центра осуществляется Центрами регистрации по обращению Клиентов, на основании представленного в письменной форме заявления о подтверждении ЭЦП Уполномоченного лица Удостоверяющего центра в сертификате (приложение №6 к настоящему Регламенту).

Обязательным приложением к заявлению о подтверждении ЭЦП Уполномоченного лица Удостоверяющего центра является внешний носитель электронной информации (дискета 3'5"), на котором записаны:

- файл сертификата зарегистрированного владельца сертификата, подвергающийся процедуре проверки;
- файл сертификата Уполномоченного лица Удостоверяющего центра, являющегося издателем сертификата зарегистрированного владельца сертификата, в достоверности которого заявитель сомневается и намерен подвергнуть процедуре проверки;
- файл списка отозванных сертификатов, издателем которого является Удостоверяющий центр, использовавшийся Клиентом-заявителем для проверки ЭЦП Уполномоченного лица Удостоверяющего центра.

Срок рассмотрения заявления о подтверждении ЭЦП Уполномоченного лица Удостоверяющего центра в сертификате составляет 5 (пять) рабочих дней с момента его представления в Центр регистрации.

По результатам проверки Клиент получает на руки протокол (Акт) проверки ЭЦП в котором содержатся:

- результат проверки ЭЦП сертифицированным средством;
- детальный отчет по выполненной проверке (экспертизе).

Детальный отчет по выполненной проверке (экспертизе) содержит следующие обязательные компоненты:

- время и место проведения проверки (экспертизы);
- основания для проведения проверки (экспертизы);
- сведения об эксперте или комиссии экспертов (фамилия, имя, отчество, занимаемая должность);
- вопросы, поставленные перед экспертом или комиссией экспертов;

- объекты исследований и материалы по заявлению, представленные эксперту для проведения проверки (экспертизы);
- содержание и результаты исследований с указанием примененных методов;
- оценка результатов исследований, выводы по поставленным вопросам и их обоснование;
- иные сведения в соответствии с Федеральным законом.

Детальный отчет составляется в письменной форме на бумажном носителе и заверяется собственноручной подписью эксперта, либо в случае формирования комиссии, подписями членов экспертной комиссии.

В случае отказа в рассмотрении заявления Клиента работник Центра регистрации вносит в его заявление свою резолюцию, раскрывающую причину отказа в рассмотрении поступившей заявки, снимает копию заявления. В оригинале заявления и в его копии Клиент ставит свою подпись, подтверждающую факт ознакомления с содержащейся в нем резолюцией работника Центра регистрации.

2.13.3 Документ, подтверждающий факт обладания электронными ключами, зарегистрированными в Удостоверяющем центре

В качестве доказательства факта обладания зарегистрированными в Удостоверяющем центре электронными ключами (ключевой пары) рассматривается бумажный документ «Бланк сертификата открытого ключа», в котором содержится следующая информация, предъявляемая в качестве доказательства владельцем электронных ключей:

- сведения о сертификате: кем выдан сертификат, кому выдан сертификат, назначение сертификата, серийный номер сертификата;
- сведения об издателе сертификата;
- информация об открытом ключе Клиента, являющегося владельцем ключевой пары, отображенная в виде цифровой последовательности идентичной значению открытого ключа в электронном сертификате владельца сертификата;
- рукописная подпись Уполномоченного лица Удостоверяющего центра заверенная печатью организации (НП «НУЦ»);

«Бланк сертификата открытого ключа» выдается на руки Клиенту (владельцу сертификата) по предъявлению с его стороны Бланка запроса на выпуск сертификата

открытого ключа (приложение №9 к настоящему регламенту), подписанного собственноручной подписью.

2.14 Представление информации о компрометации секретного (закрытого) ключа

В случае выявления фактов компрометации закрытого (секретного) ключа стороны действующего договора обязаны немедленно предпринять действия, позволяющие избежать (устранить) факты несанкционированного использования закрытого (секретного) ключа.

Удостоверяющий центр рассматривает в качестве факта компрометации закрытого (секретного) ключа Клиента следующие события:

- передача владельцем сертификата своего персонального ключевого носителя, содержащего закрытый (секретный) ключ, в пользование другому физическому лицу;
- утрата ключевого носителя владельцем сертификата, содержащего его персональный закрытый (секретный) ключ, по причине утери либо кражи ключевого носителя;
- утрата владельцем сертификата своего персонального закрытого (секретного) ключа в результате механического повреждения ключевого носителя;
- выявление владельцем персонального закрытого (секретного) ключа фактов и событий несанкционированного его использования посторонними лицами.
- изменение статуса владельца сертификата (подразумевается, что в результате произошедших изменений ранее предоставленные сведения, на основании которых был выпущен сертификат, утратили свою юридическую силу).

2.14.1 Компрометация закрытого (секретного) ключа владельца сертификата

При выявлении факта компрометации закрытого (секретного) ключа его владелец обязан:

- немедленно проинформировать работника Центра регистрации Удостоверяющего центра о факте компрометации;
- представить письменное заявление об аннулировании (отзыве) действующего сертификата с внесением сведений, раскрывающих причины компрометации сертификата.

– немедленно приостанавливать обмен электронными документами со всеми участниками информационного взаимодействия с применением ЭЦП и функций шифрования.

Клиент, объявивший о компрометации собственных криптографических ключей, обязан в течение одного рабочего дня документально оформить уведомление о произошедшем событии и направить его в Удостоверяющий центр.

Клиент может подать письменное заявление о приостановлении действия личного сертификата собственноручно, при личном прибытии в Центр регистрации, либо через доверенное лицо, на имя которого оформлена письменная доверенность, заверенная нотариусом. Форма заявления о приостановлении действия сертификата приведена в приложении №3 к настоящему Регламенту.

Порядок представления письменного заявления описан в разделах 2.9.2, 2.9.3, 2.9.4.

Срок рассмотрения заявления о приостановлении действия сертификата составляет 1 (один) рабочий день с момента приема заявления от владельца сертификата.

2.14.2 Компрометации электронных ключей Удостоверяющего центра

При компрометации электронного ключа Уполномоченного лица Удостоверяющего центра вся система Удостоверяющего центра временно приостанавливает свою работу до устранения возникшей угрозы, кроме системы предоставления информации общего доступа.

Система предоставления информации общего доступа используется Удостоверяющим центром для информирования своих Клиентов о произведенных изменениях в работе Удостоверяющего центра и о предстоящей процедуре смены электронных ключей (ключевой пары) и сертификата Уполномоченного лица Удостоверяющего центра, а также замены действующих сертификатов Клиентов.

2.15 Порядок согласования нового Регламента с Клиентом

При внесении изменений в настоящий Регламент Удостоверяющий центр публикует новый вариант Регламента на своем сайте в открытой сети Интернет. В качестве дополнительно оговариваемой услуги Удостоверяющий центр может осуществлять рассылку уведомлений о внесении изменений в настоящий Регламент.

Новый регламент вступает в силу по истечении 2 (двух) месяцев с момента его опубликования на электронном сайте Удостоверяющего центра.

Основным документом, подтверждающим намерение Клиента работать в рамках нового регламента, является дополнительное соглашение к действующему договору о присоединении к Регламенту, оформленному между Клиентом и Удостоверяющим центром.

Оформление дополнительного соглашения к действующему договору может осуществляться по следующим схемам взаимодействия:

1. Клиент в течение 2-х (двух) месячного периода, с момента опубликования нового Регламента, лично прибывает в Центр регистрации Удостоверяющего центра, в котором заключался договор о присоединении к Регламенту, для заключения дополнительного соглашения к договору (юридическое лицо для заключения дополнительного соглашения направляет своего представителя, имеющего на руках документ, подтверждающий его полномочия на совершение сделки);

2. Клиент в течение 2-х (двух) месячного периода, с момента опубликования нового Регламента присылает по электронному адресу Удостоверяющего центра свое письменное согласие, подписанное личной ЭЦП, в котором подтверждается его намерение работать в рамках нового Регламента и подтверждается выполнение принятого на себя обязательства о заключении дополнительного соглашения к действующему договору, касающегося принятия нового Регламента (по почте Клиент пересылает копию письменного согласия на бумажном носителе, заверенную личной рукописной подписью); в этом случае Удостоверяющий центр предоставляет возможность Клиенту перенести оформление дополнительного соглашения к действующему договору на момент выпуска для Клиента нового сертификата.

Если в течение 2-х (двух) месячного срока Клиент не прибыл в Удостоверяющий центр для оформления дополнительного соглашения к действующему договору, либо в Удостоверяющий центр не поступает письменное подтверждение Клиента о его намерении работать в рамках нового Регламента, Удостоверяющий центр приостанавливает все действующие сертификаты Клиента сроком на 1 (один) месяц. В течение данного периода за Клиентом сохраняется право прибыть в Центр регистрации, в котором заключался договор о присоединении к Регламенту, для оформления дополнительного соглашения к действующему договору. Если в названный период Клиент не оформляет дополнительное соглашение, договор с Клиентом считается расторгнутым, а все его сертификаты аннулируются (отзывается).

2.16 Сертификат

Сертификат открытого ключа Клиента в электронной форме представляет собой электронный документ, имеющий структуру, соответствующую стандарту Международного союза телекоммуникаций ITU-T X.509 версии 3 и рекомендаций IETF (Internet Engineering Task Force) RFC 2459 и представленный в кодировке Base64.

Ниже в подразделах текущего раздела рассмотрены структура сертификата, сроки действия сертификата в зависимости от его функционального назначения, возможные способы запроса и получения сертификата в Удостоверяющем центре, вопросы обслуживания сертификата.

2.16.1 Базовые поля сертификата

Сертификаты содержат следующие базовые поля X.509:

- Signature: ЭЦП Уполномоченного лица Удостоверяющего центра
- Issuer: Идентифицирующие данные Уполномоченного лица Удостоверяющего центра
- Validity: Даты начала и окончания срока действия сертификата
- Subject: Идентифицирующие данные владельца сертификата
- SubjectPublicKeyInformation: Идентификатор алгоритма средства ЭЦП, с которыми используется данный открытый ключ, значение открытого ключа
- Version: Версия сертификата формата X.509 - версия 3
- SerialNumber: Уникальный серийный (регистрационный) номер сертификата в Реестре сертификатов открытых ключей Удостоверяющего центра

2.16.2 Дополнения сертификата

Сертификаты содержат следующие дополнения:

- authorityKeyIdentifier: Идентификатор ключа уполномоченного лица Удостоверяющего центра
- subjectKeyIdentifier: Идентификатор ключа владельца сертификата
- ExtendedKeyUsage: Область (области) использования ключа, при которых ЭД с ЭЦП будет иметь юридическое значение

cRLDistributionPoint: Точка распространения списка аннулированных (отозванных) сертификатов открытых ключей, изданных Удостоверяющим центром

KeyUsage: Назначение ключа

2.16.3 Объектные идентификаторы алгоритма

Удостоверяющий центр использует следующие идентификаторы алгоритмов средства ЭЦП, имеющего наименование «СКЗИ КриптоПро CSP»:

Наименование	OID
ГОСТ Р 34.10-94	1.2.643.2.2.20
Диффи-Хеллмана	1.2.643.2.2.99
ГОСТ Р 34.10-2001	1.2.643.2.2.19
Диффи-Хеллмана	1.2.643.2.2.98
ГОСТ Р 34.11-94	1.2.643.2.2.9
ГОСТ 28147-89	1.2.643.2.2.21

2.16.4 Формы имени (атрибуты имени)

В сертификате поля идентификационных данных Уполномоченного лица Удостоверяющего центра и владельца сертификата содержат атрибуты имени формата X.500.

2.16.5 Ограничения на имена

Обязательными атрибутами поля идентификационных данных уполномоченного лица УЦ являются:

Common Name: Фамилия, имя, отчество

Organization: Наименование организации, являющейся владельцем Удостоверяющего центра

Organization Unit: Наименование подразделения, сотрудником которого является уполномоченное лицо Удостоверяющего центра

Email: Адрес электронной почты

Country: буквенный код страны (например, RU)

State: Субъект Федерации, где зарегистрирована организация,

являющейся владельцем Удостоверяющего центра

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего собственные интересы, являются:

Common Name: Фамилия, имя, отчество

Email: Адрес электронной почты

Country: буквенный код страны (например, RU)

Обязательными атрибутами поля идентификационных данных владельца сертификата, представляющего интересы юридического лица, являются:

Common Name: Фамилия, имя, отчество

Organization: Наименование организации, которую представляет владелец сертификата

Organization Unit: Наименование подразделения организации, сотрудником которого является владелец сертификата

Email: Адрес электронной почты

Country: буквенный код страны (например, RU)

State: Субъект Федерации, где зарегистрирована организация, которую представляет владелец сертификата

2.17 Сроки действия сертификатов

Срок действия сертификата ключа подписи составляет один год с момента его создания.

Начало периода действия электронных ключей (закрытого и открытого ключей) владельца сертификата исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа владельца сертификата.

2.17.1 Сроки действия ключей Уполномоченного лица Удостоверяющего центра

Срок действия закрытого ключа Уполномоченного лица Удостоверяющего центра составляет 1 (один) год и 3 (три) месяца. Начало периода действия закрытого ключа

Уполномоченного лица Удостоверяющего центра исчисляется с даты и времени начала действия сертификата Уполномоченного лица Удостоверяющего центра.

Срок действия сертификата соответствующего (закрытому) секретному ключу Уполномоченного лица Удостоверяющего центра составляет 6 (шесть) лет с момента начала срока действия сертификата.

2.18 Сроки хранения сертификатов в реестре

Хранение сертификатов Клиентов, зарегистрированных в реестре сертификатов Удостоверяющего центра в качестве пользователей услуг, осуществляется в течение установленного срока действия сертификата открытого ключа. Затем сертификат передается в архивное хранение.

Срок архивного хранения сертификата открытого ключа устанавливается в соответствии со сроком, определенному в разделе 2.15 настоящего Регламента.

2.19 Список отозванных сертификатов

COC (CRL) представляет собой структуру электронных данных формата X.509 v2 (версия 2), включающих в свой состав список серийных номеров аннулированных или приостановленных сертификатов, которые уникальны для сертификатов одного Удостоверяющего центра, с указанием для каждого номера сертификата времени его отзыва. В COC (CRL) обязательно указываются время его издания и время, когда будет выпущен COC (CRL) с более свежей информацией, а также адреса, по которому доступен COC (CRL). В сертификаты Клиентов Удостоверяющего центра включено дополнение - CDP (CRL Distribution Point - точка распространения COC). Таких адресов может быть несколько.

CRL подписывается цифровым методом (авторизуется) с помощью ключа подписи Уполномоченного лица Удостоверяющего центра.

Разъяснения полей информации в CRL можно найти в RFC 2459 (Internet X.509 Public Key Infrastructure Certificate and CRL profile).

COC не отражает информацию о статусах сертификатов в реальном времени

2.19.1 Основные базовые поля в COC (CRL)

Issuer: Издатель сертификата
thisUpdate: Время издания

nextUpdate: Время следующего обновления
revokedCertificates: Перечень отозванных сертификатов
CertificateSerialNumber: Серийный номер отозванного сертификата
Time: Время отзыва сертификата
SignatureAlgorithm: Алгоритм подписи издателя
IssuerSign: Подпись издателя

2.19.2 Дополнения СОС (CRL)

Удостоверяющий Центр использует следующие дополнения:

Authority Key Identifier: Идентификатор ключа Уполномоченного лица
Удостоверяющего центра
Reason Code: Код причины отзыва сертификата открытого
ключа
szOID_CERTSRV_CA_VERSION: Объектный идентификатор Microsoft Certificate
Server, определяющий версию службы
сертификации Microsoft Certification Authority

2.20 Архивное хранение документированной информации

2.20.1 Состав архивируемых документов

Архивированию подлежат следующая документированная информация:

- реестр сертификатов Клиентов Удостоверяющего центра;
- реестр сертификатов Уполномоченных лиц Удостоверяющего центра;
- реестр выпускаемых списков отозванных сертификатов;
- журналы аудита программно-аппаратных средств обеспечения деятельности Удостоверяющего центра;
- реестр Клиентов, зарегистрированных в Центре регистрации в качестве пользователей услуг Удостоверяющего центра;
- договора заключенные между Клиентом и Удостоверяющим центром
- доверенность заявителя на изготовление электронных ключей (ключевой пары) для выпущенного сертификата;

- заявления на изготовление сертификата;
- заявление о согласии с намерением работодателя;
- заявления об аннулировании (отзыве) сертификата;
- заявления о приостановлении действия сертификата;
- заявления о возобновлении действия сертификатов;
- служебные документы Удостоверяющего центра.

2.20.2 Источник комплектования архивного фонда

Источником комплектования архивного фонда Удостоверяющего центра являются подразделения (Службы) Удостоверяющего центра, обеспечивающие документирование служебной информации.

2.20.3 Архивохранилище

Архивные документы хранятся в специально оборудованном помещении-архивохранилище, обеспечивающим режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

2.20.4 Срок архивного хранения

Документы, подлежащие архивному хранению, являются документами временного хранения.

Срок хранения архивных документов – 11 лет.

2.20.5 Уничтожение архивных документов

Выделение архивных документов к уничтожению и уничтожение осуществляется постоянно действующей комиссией, формируемой из числа сотрудников Службы безопасности Удостоверяющего центра и назначаемой приказом руководителя Удостоверяющего центра.

2.21 Список приложений

Приложение №1 Форма доверенности № 1 на изготовление электронных ключей (ключевой пары).

Приложение №2 Форма копии сертификата открытого ключа на бумажном носителе.

Приложение №3 Форма заявления об аннулировании (отзыве) сертификата открытого ключа.

Приложение №4 Форма заявления о приостановлении действия сертификата открытого ключа

Приложение №5 Форма заявления о возобновлении действия сертификата открытого ключа.

Приложение №6 Форма заявления на подтверждение ЭЦП.

Приложение №7 Сертификат Уполномоченного лица Национального Удостоверяющего Центра.

Приложение №8 Форма заявления о согласии работника с намерением работодателя приобрести сертификат на имя работника.

Приложение №9 Форма приложения к Договору, содержащего список работников организации для которых необходимо выпустить сертификаты

Приложение №10 Форма доверенности № 2 на изготовление электронных ключей (ключевой пары).

Приложение №1 к Регламенту
Форма доверенности № 1 на изготовление электронных ключей (ключевой пары)

ДОВЕРЕННОСТЬ
на изготовление электронных ключей
(ключевой пары)

Я, _____
(Ф.И.О.)
паспорт серии _____ № _____ выдан _____
(где, кем, когда)

, доверяю Некоммерческому партнерству «Национальный Удостоверяющий Центр»
изготовить электронные ключи (ключевую пару) для выпущенного на мое имя сертификата

(Область применения сертификата)

Доверенность выдана на срок _____ без права передоверия
третьей стороне.

Заявитель:

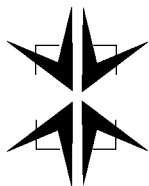
_____/Фамилия И.О./
(Подпись)
«__» _____ 200__г.

Процедуру генерации и электронных ключей (ключевой пары) выполнил:

_____/Фамилия И.О./
(Подпись)
«__» _____ 200__г.



Приложение №2 к Регламенту
Форма копии сертификата открытого ключа на бумажном носителе



НАЦИОНАЛЬНЫЙ
УДОСТОВЕРЯЮЩИЙ ЦЕНТР

некоммерческое партнерство
127018, Россия, Москва, ул. Образцова,38

СЕРТИФИКАТ

ключа подписи

Регистрационный
номер сертификата ключа подписи:

61D67FAE00000000000A

Дата начала срока действия сертификата
ключа подписи:

06.02.2007

Дата окончания срока действия
сертификата:

06.02.2008

Владельцем настоящего сертификата ключа подписи является:

T=Начальник центра отраслевых и системных проектов, Неструктурированный адрес=117393, Москва, ул.Профсоюзная, д.78, стр.4, CN=Щербина Игорь Евгеньевич, OU=Центр отраслевых и системных проектов, O=ФГУП НПП Гамма, L=Москва, ST=Центральный Федеральный Округ, C=RU, E=shepbina@nppgamma.ru

Алгоритм открытого ключа:

1.2.643.2.2.19 - ГОСТ Р 34.10-2001

Значение открытого ключа:

04 40 f7 03 ae e5 f1 c2 97 6a c8 de 94 52 79 96 d2 f1 ff df 03 e1 5e 0e d4 c6 9d 3d 04 f5 fc d0 ac 31 8c 9d a2 69 80
0a 47 c9 dd 79 42 62 34 f1 af 7f 06 a7 3e 37 e3 2f 56 50 85 d5 f5 33 78 b1 ae 95
Незначащих бит: 0

Расширения сертификата X.509:

2.5.29.15 - Использование ключа (KU), критическое расширение:

Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

2.5.29.37 - Улучшенный ключ (EKU):

1.2.643.2.2.34.6 - Клиент ЦР, 1.3.6.1.5.5.7.3.2 - Проверка подлинности клиента, 1.3.6.1.5.5.7.3.4 - Защищенная электронная почта

2.5.29.14 - Идентификатор ключа владельца:

5f b9 ea 71 be ff 57 b7 54 28 91 12 fc 43 94 d1 cc 06 ed f7

2.5.29.35 - Идентификатор ключа издателя (ЦС):

Идентификатор ключа: 89 58 06 6a 5f 7c 65 16 f8 5f 6e b0 86 f0 79 19 94 7c b6 60

2.5.29.31 - Точка распространения СОС (CDP):

URL: <http://nucrf.ru/download/ta.crl>

1.3.6.1.5.5.7.1.1 - Доступ к информации о ЦС:

Метод доступа: 1.3.6.1.5.5.7.48.2 - Доступ к информации издателей
<http://nucrf.ru/download/ta.cer>

Настоящий сертификат ключа подписи изготовлен, зарегистрирован, внесен в реестр и обслуживается
Главным удостоверяющим центром Некоммерческого партнерства "Национальный удостоверяющий центр":

CN=НП НУЦ, OU=Главной Удостоверяющий центр, O=Некоммерческое партнерство Национальный
Удостоверяющий Центр, ST=Центральный Федеральный Округ, Неструктурированный адрес=Юр.адрес:
127018; ул.Образцова; д.38, Неструктурированный адрес=Почт.адрес: 117630; ул.Старокалужское шоссе;
д.58; комн. 1424, Неструктурированное имя=Уполномоченное лицо - Щербина Игорь Евгеньевич, C=RU,
E=info@nucrf.ru

Алгоритм открытого ключа:

1.2.643.2.2.3 - ГОСТ Р 34.10-2001/ГОСТ Р 34.11-94

Значение подписи:

ca 7e 6d 95 28 62 cd 4b 9b a7 c9 8f 38 0a 8f 91 b0 dc be ae a4 8e 16 50 8f 85 3d 7c 40 6c 4f 7d 97 48 6a d5 57 ee
66 e5 83 cb dd b3 51 ef a7 fc 16 15 b4 e8 a0 d0 a7 21 be 54 9a 16 31 b4 94 88
Незначащих бит: 0

Значение открытого ключа владельца сертификата предназначено для использования со средством
криптографической защиты информации "КриптоПро CSP", версия 3.0, производства ООО "КриптоПро"
(сертификат ФСБ России от 12.09.2005 №СФ/124-0810), а также для использования с иными версиями
средств криптографической защиты информации, совместимых с версией, указанной в настоящем
сертификате, и имеющих сертификат соответствия установленным требованиям.

Электронный документ с электронной цифровой подписью, сформированной с использованием закрытого
криптографического ключа, соответствующего указанному в настоящем сертификате значению открытого
ключа, будет иметь юридическое значение при выполнении условий, предусмотренных статьей 4 пунктом 1
Федерального закона Российской Федерации от 10.01.2002 №1-ФЗ "Об электронной цифровой подписи".

Подпись уполномоченного лица
удостоверяющего центра:

_____ (_____)

М.П.

Подпись
владельца сертификата:

_____ (_____)

Приложение №3 к Регламенту
Форма заявления об аннулировании (отзыве) сертификата открытого ключа

ЗАЯВЛЕНИЕ
об аннулировании (отзыве) сертификата

Прошу аннулировать (отозвать) действующий сертификат, серийный номер: _____

_____ выданный на имя _____
(Ф.И.О. владельца сертификата)

_____ начиная с _____
(дата аннулирования)

Причина аннулирования (отзыва) сертификата: _____

Заявитель:

является _____
(статус заявителя)

_____ /Фамилия И.О./
(Подпись)

«___» _____ 200__ г.

Настоящим подтверждаю, что Заявление о приостановлении действия сертификата получено, личность заявителя идентифицирована, сведения, указанные в Заявлении проверены.

Представитель Центра регистрации:

_____ /Должность/
_____ /Фамилия И.О./
(Подпись)

«___» _____ 200__ г.

Приложение №4 к Регламенту

Форма заявления о приостановлении действия
сертификата открытого ключа

ЗАЯВЛЕНИЕ

о приостановлении действия сертификата

Прошу приостановить действие сертификата, серийный номер: _____

_____ выданного на имя _____
(Ф.И.О. владельца сертификата)

_____ на срок _____ календарных дней

с _____ 20__ г. по _____ 20__ г.

Причина приостановления действия сертификата: _____

Заявитель:

является _____
(статус заявителя)

_____/Фамилия И.О./
(Подпись)

«___» _____ 200__ г.

Настоящим подтверждаю, что Заявление о приостановлении действия сертификата получено, личность заявителя идентифицирована, сведения, указанные в Заявлении проверены.

Представитель Центра регистрации:

_____/Должность/
_____/Фамилия И.О./
(Подпись)

«___» _____ 200__ г.

Приложение №5 к Регламенту

Форма заявления о возобновлении действия сертификата открытого ключа

ЗАЯВЛЕНИЕ

о возобновлении действия сертификата

Прошу возобновить действие сертификата, серийный номер: _____

_____ выданного на имя _____
(Ф.И.О. владельца сертификата)

_____ начиная с _____
(дата активации)

Заявитель:

является _____
(статус заявителя)

_____/Фамилия И.О./
(Подпись)

Настоящим подтверждаю, что Заявление о возобновлении действия сертификата получено, личность заявителя идентифицирована, сведения, указанные в Заявлении проверены.

Представитель Центра регистрации:

_____/Должность/
_____/Фамилия И.О./
(Подпись)

«___» _____ 200__г.

Приложение №6 к Регламенту

Форма заявления на подтверждение ЭЦП

ЗАЯВЛЕНИЕ НА ПОДТВЕРЖДЕНИЕ ЭЦП

(в электронном документе/Уполномоченного лица Удостоверяющего центра)

Прошу подтвердить подлинность ЭЦП в файле электронного документа/сертификате

(ненужное зачеркнуть)

_____ (именование лица, чью подпись необходимо проверить)

серийный номер сертификата _____

выданного на имя _____

(Ф.И.О. владельца сертификата)

и установить статус этого сертификата в момент времени _____

(Дата и время)

К заявлению прилагаются: _____

(Перечень прилагаемого материала)

Заявитель:

_____/Фамилия И.О./

(Подпись)

«___» _____ 200__ г.



Приложение №7 к Регламенту
Сертификат Уполномоченного лица Национального Удостоверяющего Центра

СЕРТИФИКАТ
КЛЮЧА ПОДПИСИ

Регистрационный номер сертификата ключа подписи: 61 75 60 f3 00 00 00 00 00 0b

Дата начала срока действия сертификата ключа подписи: 13 сентября 2007 г.

Дата окончания срока действия сертификата: 13 сентября 2010 г.

Владельцем настоящего сертификата ключа подписи является:

Неструктурированное имя=Уполномоченное лицо - Щербина Игорь Евгеньевич, Неструктурированный адрес=Юр.адрес: 127018, ул.Образцова, д.38, Неструктурированный адрес=Почт.адрес: 117630, ул.Старокалужское шоссе, д.58, комн. 1424, CN=НП НУЦ (ВЕУЦ), OU=Восточно-Европейский Удостоверяющий центр, O=Некоммерческое партнерство Национальный Удостоверяющий Центр, L=Москва, ST=Центральный Федеральный Округ, C=RU, E=info@nucrf.ru

* В сертификате ключа подписи (значение поля CN) использован псевдоним

Алгоритм открытого ключа: ГОСТ Р 34.10-2001 (1.2.643.2.2.19)

Параметры открытого ключа: ГОСТ Р 34.10-2001, параметры по умолчанию (1.2.643.2.2.35.1)

Параметры хэш-функции: ГОСТ Р 34.11-94, параметры по умолчанию (1.2.643.2.2.30.1)

Идентификатор ключа субъекта (2.5.29.14): 48 b4 d2 54 54 7b 41 cf 98 33 07 be 46 3c cd e7 d4 92 04 d2

Значение открытого ключа:

04 40 24 32 c7 b2 43 0a 87 bb 43 ed 0f 40 cb d1 58 4d 66 94 17 05 10 5c ce fa 61 99 50 41 90 7c 71 83 8f f5 c3
14 43 9b 8b 41 98 80 6f 85 73 8f 3a be f8 f0 80 61 5f 1f 65 7c 28 13 80 76 7b 66 01 ce
Незначащих бит: 0

Настоящий открытый ключ электронной цифровой подписи предназначен для использования со средством криптографической защиты информации (средством электронной цифровой подписи) «КриптоПро-СРП», версии 3.0, производства ООО «Крипто-Про» (сертификат ФСБ России от 12.09.2005 № СФ/124-0810), а также иными средствами, совместимыми с указанным, и имеющими сертификат соответствия установленным требованиям.

Использование ключа (2.5.29.15):

Цифровая подпись; Подписание сертификатов; Подписывание списка отзыва (CRL) (86)



Основные ограничения (2.5.29.19) (критическое расширение):

Тип субъекта = ЦС; Ограничение на длину пути = 0

Политика сертификата:

Идентификатор политики = 1.2.643.3.46.10.1; Идентификатор квалификатора политики = Уведомление пользователя; Текст уведомления = Сертификат предназначен для применения уполномоченными лицами корневых Удостоверяющих центров, обеспечивающих выполнение требований УФО; Идентификатор квалификатора политики = CPS; CPS = <http://nucrf.ru/download/ta-policy.html>
Идентификатор политики = 1.2.643.3.46.10.3; Идентификатор квалификатора политики = Уведомление пользователя; Текст уведомления = Сертификат предназначен для формирования сертификатов конечным пользователям услуг Некоммерческого партнерства Национальный Удостоверяющий Центр; Идентификатор квалификатора политики = CPS; CPS = <http://nucrf.ru/download/ta-policy.html>

Настоящий сертификат ключа подписи изготовлен, зарегистрирован, внесен в реестр и обслуживается Главным удостоверяющим центром Некоммерческого партнерства «Национальный удостоверяющий центр»

CN=НП НУЦ, OU=Главной Удостоверяющий центр, O=Некоммерческое партнерство Национальный Удостоверяющий Центр, ST=Центральный Федеральный Округ, L=Москва, Неструктурированный адрес=Юр.адрес: 127018, ул.Образцова, д.38, Неструктурированный адрес=Почт.адрес: 117630, ул.Старокалужское шоссе, д.58; комн. 1424, 1.2.840.113549.1.9.2=Уполномоченное лицо - Щербина Игорь Евгеньевич, C=RU, E=info@nucrf.ru

Юридический адрес удостоверяющего центра:

Юр.адрес: 127018; ул.Образцова; д.38

Почтовый адрес (для переписки) удостоверяющего центра:

Почт.адрес: 117630; ул.Старокалужское шоссе; д.58; комн. 1424

Идентификатор ключа издателя (ЦС):

Идентификатор ключа: 54 9f e7 ae 87 89 80 c2 2a 75 3e 8b b2 dc 42 4e 56 4e ea 0a

Доступ к сведениям удостоверяющего центра (1.3.6.1.5.5.7.48):

Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) – Доступ к информации издателей;
URL = <http://nucrf.ru/download/ta0.cer>

Точка распространения списка отозванных сертификатов (CRL) (2.5.29.31):

URL = <http://nucrf.ru/download/ta0.crl>

Алгоритм открытого ключа:

ГОСТ Р 34.10-2001
(1.2.643.2.2.19)

Значение подписи:

e4 5c 47 a2 94 f6 5c 74 b1 24 eb 0c 13 d0 56 a3 d3 64 e8 b7 70 c7 70 1f 7c e4 7b 1e 23 1a 51 6f 57 cf 74 e4 f0 5e cd 44 56 b3 fa 9d fa f1 af 55 3c 47 8e d7 81 1a fe 00 96 0d 11 af e5 c6 a7 f9
Незначащих бит: 0

Настоящий сертификат ключа подписи выдан в отношении открытого ключа электронной цифровой подписи уполномоченного лица удостоверяющего центра.

Электронная цифровая подпись уполномоченного лица удостоверяющего центра может быть использована только после включения в единый государственный реестр соответствующего сертификата

ключа подписи.

Использование электронной цифровой подписи уполномоченного лица удостоверяющего центра для целей, не связанных с заверением сертификатов ключей подписей и сведений об их действии, не допускается.

Подпись уполномоченного лица
удостоверяющего центра:

_____/_____
(подпись) (расшифровка Ф.И.О.)

М.П. "___" _____ 200__ г.

Подпись руководителя
удостоверяющего центра:

_____/_____
(подпись) (расшифровка Ф.И.О.)

М.П. "___" _____ 200__ г.



Приложение №9 к Регламенту

Форма приложения к Договору, содержащего список работников организации для которых необходимо выпустить сертификаты

Приложение № ____
к Договору от _____ № _____

Директору Некоммерческого партнерства
«Национальный Удостоверяющий Центр»
Щербине И.Е.

СПИСОК РАБОТНИКОВ для выпуска сертификатов

В рамках заключенного договора о присоединении к Регламенту
между

(Полное название организации)

и Некоммерческим партнерством «Национальный Удостоверяющий Центр» прошу
выпустить сертификаты для следующих работников:

№ п.п.	ФИО (полностью)	Должность	Адрес электронной почты (e-mail)

Руководитель организации:

/Фамилия И.О./

(Подпись)

«___» _____ 200__ г.

М.П.

Приложение №10 к Регламенту

Форма доверенности № 2 на изготовление электронных ключей (ключевой пары)

ДОВЕРЕННОСТЬ № _____

Дата выдачи «___» _____ 200__ г.

Действительна по «___» _____ 200__ г.

Я,

(ФАМИЛИЯ Имя Отчество)

(Должность, название организации)

Паспорт

(Серия)

(Номер)

Кем выдан

Дата выдачи

ДОВЕРЯЮ

(ФАМИЛИЯ Имя Отчество)

(Должность, название организации)

Паспорт

(Серия)

(Номер)

Кем выдан

Дата выдачи

ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

вместо меня присутствовать при создании ключей моей электронной цифровой подписи (ЭЦП) и сертификата ключа подписи;

получить ключевой носитель, содержащий:

- ключевые файлы в контейнере;
- сертификат ключа подписи;

получить мой сертификат ключа подписи;

расписаться за меня в Сертификате ключа подписи и актах;

подписать за меня финансовые документы (в рамках выполненных работ и оказанных услуг).

Подпись лица, получившего доверенность

(подпись)

(Фамилия И.О.)

Подпись лица, выдавшего доверенность

(подпись)

(Фамилия И.О.)

УДОСТОВЕРЯЮ

(Должность руководителя, название организации)

(подпись)

(Фамилия И.О.)

М.П.

«___» _____ 200__ г.

