Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕН
приказом от 26.06.2020 № 12

Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (Регламент Удостоверяющего центра InfoTrust, Certification Practice Statement — CPS)

OID 1.2.643.3.34.1.1

Редакция № 8

INFOTRUST
удостоверяющий центр

Ижевск 2020

Реферат

Настоящий документ содержит Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее — Регламент, Регламент Удостоверяющего центра InfoTrust) ООО Научно-производственное предприятие «Ижинформпроект».

Регламент удостоверяющего центра создан в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», приказа Минкомсвязи России от 13.08.2018 № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей», с учетом рекомендаций RFC 3647 «Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework» и содержит порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

Содержание

стр.
1 Определения 7
2 Обозначения и сокращения 15
3 Общие положения 17
3.1 Предмет регулирования Регламента 17
3.2 Сведения об Удостоверяющем центре 17
3.3 Порядок информирования о предоставлении услуг Удостоверяющего центра 21
3.4 Идентификация Регламента 21
3.5 Применение Регламента 22
3.6 Изменения (дополнения) Регламента 22
3.7 Взаимозависимости Регламента 23
3.8 Стоимость услуг Удостоверяющего центра 24
4 Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг) 26
5 Предоставление информации 28
5.1 Удостоверяющий центр 28
5.2 Сторона Договора 28
6 Права и обязанности 31
6.1 Обязанности Удостоверяющего центра 31
6.2 Обязанности Стороны Договора 34
6.3 Обязанности Пользователя УЦ 34
6.4 Права Удостоверяющего центра 35
6.5 Права Стороны Договора 37
6.6 Права Пользователя УЦ 37
7 Ответственность сторон 39
8 Разрешение споров 41
9 Конфиденциальность информации 42
9.1 Типы конфиденциальной информации 42

9.2 Типы информации, не являющейся конфиденциальной 42
9.3 Исключительные полномочия Удостоверяющего центра 42
9.4 Обработка персональных данных Пользователей УЦ 42
10 Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в Удостоверяющий центр в рамках предоставления услуг 46
10.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей 46
10.2 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра 49
10.3 Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности 50
10.4 Процедура создания и выдачи квалифицированных сертификатов (с регистрацией Пользователя УЦ) 52
10.5 Процедура создания и выдачи квалифицированных сертификатов (без регистрации Пользователя УЦ) 59
10.6 Информация о сертификатах ключей уполномоченного лица Удостоверяющего центра 62
10.7 Компрометация ключа Пользователя УЦ 62
10.8 Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата 62
10.9 Получение информации о статусе сертификата, изданного Удостоверяющим центром 65
10.10 Подтверждение действительности электронной подписи, использованной для подписания электронных документов 66
10.11 Порядок ведения реестра квалифицированных сертификатов 68
10.12 Порядок технического обслуживания реестра квалифицированных сертификатов 69

10.13 Предоставление Удостоверяющим центром сервиса Службы актуальных статусов сертификатов ____ 70
10.14 Предоставление Удостоверяющим центром сервиса Службы штампов времени ____ 71
10.15 Предоставление Удостоверяющим центром услуг системы «КриптоСвязь»{Защищенный Электронный Документооборот} ____ 73
11 Порядок исполнения обязанностей Удостоверяющего центра ____ 74
12 Сроки действия ключевых документов ____ 77
13 Структура сертификатов и списков отозванных сертификатов ____ 79
13.1 Структура сертификата уполномоченного лица Удостоверяющего центра ____ 79
13.2 Структура списка отозванных сертификатов ____ 81
13.3 Структура сертификата Пользователя УЦ ____ 81
14 Дополнительные положения ____ 84
14.1 Прекращение оказания услуг Удостоверяющим центром ____ 84
14.2 Хранение сертификатов в Удостоверяющем центре ____ 84
14.3 Хранение документов в Удостоверяющем центре ____ 84
15 Форс-мажор ____ 85
Приложение А Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ЮЛ) ____ 86
Приложение Б Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ИП/ФЛ) ____ 90
Приложение В Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ИС) ____ 93
Приложение Г Заявление об изготовлении сертификата Пользователя Удостоверяющего центра InfoTrust ____ 96
Приложение Д Заявление об аннулировании (отзыве) сертификата Пользователя Удостоверяющего центра InfoTrust ____ 98
Приложение Е Заявление об отзыве/прекращении полномочий Пользователя Удостоверяющего центра InfoTrust ____ 99

Приложение Ж Заявление о получении информации о статусе сертификата, изготовленного Удостоверяющим центром InfoTrust 100
Приложение И Заявление о подтверждении действительности электронной подписи, использованной для подписания электронных документов 101
Приложение К Заявление о замене номера телефона Пользователя Удостоверяющего центра InfoTrust 102
Приложение Л Копия сертификата на бумажном носителе 103
16 Лист регистрации изменений 104

1 Определения

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

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

Сертификат средств электронной подписи — документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной подписи установленным требованиям.

Электронная подпись — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Ключ электронной подписи (закрытый ключ) — уникальная последовательность символов, предназначенная для создания электронной подписи.

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

Сертификат ключа проверки электронной подписи (сертификат) — электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и

подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

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

Сертификат в форме документа на бумажном носителе — документ на бумажном носителе, содержащий информацию из сертификата и заверенный собственноручной подписью уполномоченного лица Удостоверяющего центра и печатью Удостоверяющего центра. Стороны признают возможность использования факсимиле подписи (клише с подписи) уполномоченного лица Удостоверяющего центра для подписи сертификата в качестве аналога собственноручной подписи, равнозначного собственноручной подписи.

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

Владелец сертификата ключа проверки электронной подписи (*владелец сертификата)* — лицо, которому в установленном Федеральным законом «Об электронной подписи» порядке выдан сертификат ключа проверки электронной подписи.

Псевдоним владельца сертификата — вымышленное имя владельца сертификата, которое он сознательно и легально принимает для регистрации в Удостоверяющем центре.

Удостоверяющий центр — Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект», осуществляющий выполнение целевых функций Удостоверяющего центра в соответствии с Федеральным законом «Об электронной подписи» непосредственно и/или через Регистрационные отделения Удостоверяющего центра (перечень публикуется на сайте www.infotrust.ru).

Аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям Федерального закона «Об электронной подписи».

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

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

— реестр заявлений на регистрацию в Удостоверяющем центре;

— реестр зарегистрированных пользователей Удостоверяющего центра;

— реестр заявлений на создание сертификата;

— реестр заявлений на аннулирование (отзыв) сертификата;

— реестр заявлений на приостановление/возобновление действия сертификата;

— реестр заявлений на подтверждение подлинности электронной подписи в электронном документе;

— реестр заявлений на подтверждение электронной подписи уполномоченного лица Удостоверяющего центра в изданных сертификатах;

— реестр сертификатов;

— реестр созданных списков отозванных сертификатов.

Уполномоченное лицо Удостоверяющего центра — физическое лицо, являющееся сотрудником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов и списков отозванных сертификатов.

Регистрационное отделение Удостоверяющего центра (Регистрационное отделение) — подразделение Удостоверяющего центра, юридическое лицо или индивидуальный предприниматель, заключившее с Удостоверяющим центром договор, уполномоченное Удостоверяющим центром осуществлять регистрацию Пользователей УЦ, в т.ч.:

— взаимодействие с Пользователем УЦ, информирование и обработка (прием, регистрация, выдача) документов, предусмотренных Регламентом;

— идентификация получателя сертификата (заявителя) либо полномочий лица, выступающего от имени заявителя, по обращению за получением данного сертификата в соответствии с Регламентом УЦ, проверка атрибутов и полномочий должностных лиц, подготовка и занесение регистрационной информации Пользователя УЦ в Реестр Удостоверяющего центра.

Инфраструктура открытых ключей (ИОК) / Public Key Infrastructure (PKI) — технологическая инфраструктура и сервисы, гарантирующие безопасность информационных и коммуникационных систем, использующих криптографические алгоритмы с открытыми ключами.

Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей/Регламент Удостоверяющего центра/Регламент/ Certification Practice Statement (CPS) — документ, устанавливающий общий порядок и условия предоставления Удостоверяющим центром услуг по созданию и выдаче сертификатов и дополнительных услуг, связанных с управлением сертификатами.

Правила применения сертификатов (ППС)/ Certificate policy (CP) — установленный набор правил, характеризующих возможность применения сертификата определенным сообществом и/или для класса приложений с определенными требованиями безопасности. Правила применения сертификатов позволяет доверяющей стороне оценить надежность использования сертификата для определенного приложения.

Информационно-телекоммуникационная система (Система) — корпоративная информационная система, устроителем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых

ключей (ИОК, PKI), в которой используются сертификаты, созданные Удостоверяющим центром, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы.

Организатор / Оператор / Владелец Системы — устроитель корпоративной информационной системы с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Сторона Договора/ Абонент / Участник Системы — юридическое или физическое лицо, участник информационного обмена электронными документами, зарегистрированный в Системе, и при необходимости имеющий с Организатором Системы договорные отношения о присоединении к Системе, соблюдающий требования и условия пользования Системой (в том числе применения электронной подписи), и признающий настоящий Регламент.

Пользователь Удостоверяющего центра (Пользователь УЦ) — физическое лицо, зарегистрированное в Удостоверяющем центре и являющееся уполномоченным представителем *Абонента (Участника) Системы*.

Участники электронного взаимодействия — осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, индивидуальные предприниматели, а также граждане.

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

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

Рабочий день Удостоверяющего центра (рабочий день) — промежуток времени с 10:00 до 17:00 по Ижевскому времени (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4) каждого дня недели за исключением выходных и праздничных дней.

Рассмотрение заявления на аннулирование (отзыв) сертификата, приостановление/возобновление действия сертификата — принятие ответственным лицом Удостоверяющего центра решения об осуществлении обработки заявления на основе предоставленных Пользователей УЦ документов.

Обработка заявления на аннулирование (отзыв) сертификата, приостановление/возобновление действия сертификата — совокупность действий по занесению сведений об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата в реестр Удостоверяющего центра и уведомлению пользователя об аннулировании (отзыве) сертификата, приостановлении/возобновлении действия сертификата.

Вручение сертификата ключа проверки электронной подписи — передача *Удостоверяющим центром* созданного сертификата его владельцу.

Подтверждение владения ключом электронной подписи — получение *Удостоверяющим центром* доказательств того, что лицо, обратившееся за получением сертификата, владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному таким лицом для получения сертификата.

Заявитель — коммерческая организация, некоммерческая организация, индивидуальный предприниматель, физическое лицо, не зарегистрированное в качестве индивидуального предпринимателя, но осуществляющее профессиональную деятельность, приносящую доход, в соответствии с федеральными законами на основании государственной регистрации и (или) лицензии, в силу членства в саморегулируемой организации, а также любое иное физическое лицо, лица, замещающие государственные должности Российской Федерации или государственные должности субъектов Российской Федерации, должностные лица государственных органов, органов местного самоуправления, работники подведомственных таким органам организаций, нотариусы и уполномоченные на совершение нотариальных действий лица, обращающиеся с соответствующим заявлением на выдачу сертификата ключа проверки электронной

подписи в удостоверяющий центр за получением сертификата ключа проверки электронной подписи в качестве будущего владельца такого сертификата.

Оператор Службы актуальных статусов сертификатов — ответственный сотрудник *Удостоверяющего центра*, являющийся владельцем сертификата и соответствующего закрытого ключа, с использованием которого подписываются электронной подписью электронные ответы Службы актуальных статусов сертификатов.

Оператор Службы штампов времени — ответственный сотрудник *Удостоверяющего центра*, являющийся владельцем сертификата, с использованием которого подписываются электронной подписью штампы времени.

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

Cryptographic Message Syntax (CMS) — стандарт, определяющий формат и синтаксис криптографических сообщений (RFC 5652).

CMS Advanced Electronic Signatures (CAdES) — формат усовершенствованной электронной подписи типа CAdES-X Long Type 1 в соответствии ETSI TS 101 733 «Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)» с учётом использования российских криптографических алгоритмов и RFC 5126.

Internet Protocol Security (IPsec) & Internet Key Exchange (IKE) — группа протоколов криптографической защиты на сетевом уровне (RFC 6071).

Online Certificate Status Protocol (OCSP) — протокол установления статуса сертификата открытого ключа (RFC 2560).

Public Key Cryptography Standards (PKCS) — стандарты криптографии с открытым ключом, разработанные компанией RSA Data Security. Удостоверяющий центр осуществляют свою работу в соответствии со следующими стандартами PKCS:

— *PKCS#7* — стандарт, определяющий формат и синтаксис криптографических сообщений.

— *PKCS#10* — стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа.

Secure/Multipurpose Internet Mail Extensions (S/MIME) — формат сообщений защищенной электронной почты (RFC 5751).

Time-Stamp Protocol (TSP) — протокол получения штампа времени (RFC 3161)».

The Transport Layer Security (TLS) Protocol — протокол криптографической защиты на транспортном уровне (RFC 5246).

2 Обозначения и сокращения

CAdES	CMS Advanced Electronic Signatures (Формат усовершенствованной электронной подписи)
CDP	CRL Distribution Point (Точка распространения СОС)
CMS	Cryptographic Message Syntax (Синтаксис криптографических сообщений)
CP	Certificate Policy (Правила применения сертификатов)
CPS	Certification Practice Statement (Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей/Регламент Удостоверяющего центра/Регламент)
CRL	Certificate Revocation List (Список отозванных сертификатов)
DN	Distinguished Name (Отличительное имя)
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security (Протокол криптографической защиты на сетевом уровне)
OID	Object IDentifier (Объектный идентификатор)
OCSP	Online Certificate Status Protocol (Протокол установления актуального статуса сертификата)
PDS	PKI Disclosure Statement (Справочник по ИОК УЦ)
PKI	Public Key Infrastructure (Инфраструктура Открытых Ключей)
RFC	Request For Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions (Формат сообщений защищенной электронной почты)
TLS	Transport Layer Security Protocol (Протокол криптографической защиты на транспортном уровне)
TSP	Time-Stamp Protocol (Протокол получения штампа времени)
URI	Uniform Resource Identifier (Единый идентификатор ресурса)
URL	Uniform Resource Locator (Единый локатор ресурса)

UTC/GMT	Universal Time Coordinated/Greenwich Mean Time (Универсальное координированное время/Всемирное время «по Гринвичу»)
ИОК	Инфраструктура Открытых Ключей (Public Key Infrastructure)
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат)
КС	Квалифицированный сертификат (Квалифицированный сертификат ключа проверки электронной подписи)
КЭП	Квалифицированная электронная подпись
НСД	Несанкционированный доступ
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКПЭП	Сертификат ключа проверки электронной подписи
СОС	Список отозванных сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЭП	Электронная подпись

3 Общие положения

3.1 Предмет регулирования Регламента

Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (далее — Регламент Удостоверяющего центра InfoTrust, Регламент) разработан в соответствии с действующим законодательством Российской Федерации, регулирующим деятельность удостоверяющих центров, и устанавливает общий порядок и условия предоставления *Удостоверяющим центром Абоненту Системы* услуг по созданию сертификатов и дополнительных услуг, связанных с управлением сертификатами, включая права, обязанности и ответственность *Удостоверяющего центра*.

Настоящий Регламент распространяется:

— в форме электронного документа по адресу: www.infotrust.ru.

— в форме документа на бумажном носителе (за вознаграждение, установленное настоящим Регламентом).

3.2 Сведения об Удостоверяющем центре

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги аккредитованного удостоверяющего центра в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», именуемое в дельнейшем «*Удостоверяющий центр*», зарегистрировано на территории Российской Федерации в городе Ижевске.

Удостоверяющий центр InfoTrust формирует сертификаты ключей проверки электронной подписи (далее – сертификаты) и списки отозванных сертификатов в соответствии с Рекомендациями ITU-T X.509 «Information Technology — Open Systems Interconnection — The Directory: Authentication Framework», RFC 5280 «Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile» и RFC 3039 «Internet X.509 Public Key Infrastructure Qualified

Certificates Profile» с соблюдением требований Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Приказа ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Удостоверяющий центр осуществляет свою деятельность на территории Российской Федерации на основании следующих лицензий:

1 лицензия Управления ФСБ России по Удмуртской Республике на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) от 11.10.2016 № 110Н;

2 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации, от 18.08.2018 № 163770;

3 лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2018 № 163771.

Сертификаты уполномоченного лица *Удостоверяющего центра* зарегистрированы в Едином государственном реестре сертификатов ключей подписей уполномоченных лиц удостоверяющих центров, о чем получены соответствующие уведомления Минкомвязи России (Росинформтехнологии):

1 Уведомление № 40 от 13 апреля 2006 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Регистрационный номер записи № П44-05-12-32 от 16.03.2006;

2 Уведомление № 136 от 05 октября 2007 г. о регистрации сертификата ключа подписи уполномоченного лица Удостоверяющего центра. Регистрационный номер записи № П44-05-12-134 от 03.10.2007;

3 Уведомление № 324 от 28 сентября 2009 г. о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Регистрационный номер записи № П44-05-12-324 от 28.09.2009;

4 Уведомление № 767 от 04 октября 2011 г. о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров. Регистрационный номер записи № П44-05-12-767 от 04.10.2011;

5 Уведомление Минкомсвязи от 16.08.2012 № 996 о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров;

6 Уведомление Минкомсвязи от 09.10.2012 № 1015 о внесении в Единый государственный реестр сертификатов ключей подписей уполномоченных лиц удостоверяющих центров.

Сертификаты ключа подписи уполномоченного лица *Удостоверяющего центра* включены в Список доверенных удостоверяющих центров общероссийского государственного информационного центра на основании Заключения по итогам оценки соответствия удостоверяющего центра ООО НПП «Ижинформпроект» Требованиям к технологиям, форматам, протоколам информационного

взаимодействия, унифицированным программно-техническим средствам подсистемы удостоверяющих центров общероссийского государственного информационного центра (направлено письмом Росинформтехнологии № П44-438 от 08.12.2009, продлено до 30.11.2011).

Удостоверяющий центр InfoTrust присоединен к единой системе удостоверяющих центров в области электронной цифровой подписи:

1 Свидетельство Минкомвязи России № 146 от 10 ноября 2011 г. о присоединении к Единой системе удостоверяющих центров в области электронной цифровой подписи.

Удостоверяющий центр InfoTrust аккредитован в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»:

1 Свидетельство Минкомвязи России № 17 от 19 июля 2012 об аккредитации удостоверяющего центра (на основании Приказа Минкомсвязи России № 182 от 19.07.2012 «Об аккредитации удостоверяющих центров»);

2 Свидетельство Минкомвязи России № 794 от 21 августа 2017 об аккредитации удостоверяющего центра (на основании Приказа Минкомсвязи России № 427 от 21.08.2017 «Об аккредитации удостоверяющих центров»).

Реквизиты ООО НПП «Ижинформпроект»:

ИНН 1831014533 КПП 183101001 ОГРН 1021801161140

Юридический адрес: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Фактическое местонахождение: ул. Бородина, 21, офис 207, г. Ижевск, Удмуртская Республика, 426057

Банковские реквизиты:

Удмуртское отделение № 8618 ПАО СБЕРБАНК г. Ижевск

р/с 40702810768170101530

к/с 30101810400000000601

БИК 049401601

График работы:

С 09:00 до 13:00 и с 14:00 до 18:00 по Ижевскому времени (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4) каждого дня недели за исключением выходных и праздничных дней.

3.3 Порядок информирования о предоставлении услуг Удостоверяющего центра

Контактная информация:

справочный телефон (телефон-автоинформатор): +7 (3412) 918-100,

адрес электронной почты: pki@infotrust.ru,

адрес сайта: www.infotrust.ru.

Порядок получения информации заявителями по вопросам предоставления услуг *Удостоверяющего центра* публикуется на сайте *Удостоверяющего центра* по адресу www.infotrust.ru. Любые справки по вопросам, связанным с предоставлением услуг *Удостоверяющего центра*, предоставляются сотрудниками *Удостоверяющего центра* по телефону +7 (3412) 918-100 (в рабочее время) и по адресу электронной почты pki@infotrust.ru.

3.4 Идентификация Регламента

Наименование документа — Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (Регламент удостоверяющего центра InfoTrust).

Наименование на английском языке — Certification Practice Statement (CPS).

Версия: 8.

Дата: 26.06.2020.

Объектный идентификатор: 1.2.643.3.34.1.1

Количество страниц в документе: 106.

3.5 Применение Регламента

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

В случае противоречия и/или расхождения названия какой-либо статьи со смыслом какого-либо пункта в ней содержащегося, Стороны считают доминирующим смысл и формулировки каждого конкретного пункта.

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

3.6 Изменения (дополнения) Регламента

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

Уведомление *Абонента Системы* о внесении изменений (дополнений) в Регламент осуществляется *Удостоверяющим центром* путем размещения указанных изменений (дополнений) на сайте *Удостоверяющего центра* по адресу www.infotrust.ru.

Все изменения (дополнения), вносимые *Удостоверяющим центром* в Регламент и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для Сторон по истечении 30 (тридцати) календарных дней с момента размещения указанных изменений и дополнений в Регламенте на сайте *Удостоверяющего центра* www.infotrust.ru.

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

Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех Пользователей УЦ и *Абонентов Системы*.

3.7 Взаимозависимости Регламента

Настоящий Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей (Регламент Удостоверяющего центра InfoTrust, Certification Practice Statement — CPS), OID 1.2.643.3.34.1.1, имеет соответствующие взаимные зависимости со следующими документами:

— Правила применения сертификатов Удостоверяющего центра InfoTrust (Certificate Policy — CP) — регламентируют применение сертификата для разрешенных приложений и систем с установленными требованиями безопасности, OID 1.2.643.3.34.1.2;

— Справочник по Инфраструктуре открытых ключей Удостоверяющего центра InfoTrust (PKI Disclosure Statement — PDS)— описывает основные условия получения сертификатов в Удостоверяющем центре и порядок их использования в различных приложениях Инфраструктуры открытых ключей, OID 1.2.643.3.34.1.3;

— Положение об Удостоверяющем центре InfoTrust (Certification Authority Regulations) — определяет организационную структуру, технические требования к оборудованию и программному обеспечению Удостоверяющего центра, устанавливающий требования к организационным, инженерно-техническим, программно-аппаратным методам обеспечения информационной безопасности, OID 1.2.643.3.34.1.4 (конфиденциально);

— Прейскурант на услуги Удостоверяющего центра InfoTrust, (Price List) — содержит данные о стоимости услуг Удостоверяющего центра, OID 1.2.643.3.34.1.5;

— Перечень объектных идентификаторов ООО НПП «Ижинформпроект» (OID index) — содержит зарегистрированные объектные идентификаторы (OID) соответствующих сфер применения и профилей сертификатов, OID 1.2.643.3.34.1.6;

— Регламент системы «КриптоСвязь»{Защищенный Электронный Документооборот} ООО Научно-производственное предприятие «Ижинформпроект» — определяет порядок взаимодействия участников системы;

— Порядок использования квалифицированной электронной подписи — информирует об условиях и о порядке использования электронных подписей и

средств электронной подписи, о рисках, связанных с использованием электронных подписей;

— Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи — информирует о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки;

— Договор предоставления услуг удостоверяющего центра;

— Документы (договоры, положения, соглашения, регламенты и т.п.), регламентирующие порядок взаимодействия *Абонентов Системы* и/или *Пользователей УЦ* в Информационно-телекоммуникационной системе, основанной на технологии *Инфраструктуры открытых ключей (ИОК, PKI)*, и порядок использования в ней сертификатов, выпущенных *Удостоверяющим центром* InfoTrust.

3.8 Стоимость услуг Удостоверяющего центра

Вознаграждение *Удостоверяющего центра* по настоящему Регламенту устанавливается в соответствии с Прейскурантом на услуги *Удостоверяющего центра.* Действующий Прейскурант цен можно получить в офисе *Удостоверяющего центра* или загрузить с сервера *Удостоверяющего центра* www.infotrust.ru.

Порядок информирования заинтересованных лиц о стоимости услуг *Удостоверяющего центра*, сроках и порядке расчетов за оказание услуг *Удостоверяющего центра* публикуется на сайте *Удостоверяющего центра* по адресу www.infotrust.ru. Любые справки по вопросам, связанным с предоставлением услуг *Удостоверяющего центра*, предоставляются сотрудниками *Удостоверяющего центра* по телефону +7 (3412) 918-100 (в рабочее время) и по адресу электронной почты pki@infotrust.ru.

В случае выполнения внеплановой смены ключей уполномоченного лица *Удостоверяющего центра Удостоверяющий центр* выполняет создание сертификатов *Пользователей УЦ* безвозмездно.

Оплата осуществляется на основании счета на оплату в российских рублях в безналичном порядке с использованием платежных поручений, или иным способом, предусмотренным законодательством Российской Федерации.

Сторона Договора, вносит аванс в размере 100% стоимости услуг, оказываемых *Удостоверяющим центром,* в соответствии размером вознаграждения, установленным настоящим *Регламентом.*

По согласованию с *Организатором Системы* сроки, условия и порядок расчетов могут быть изменены.

4 Перечень реализуемых Удостоверяющим центром функций (оказываемых услуг)

— создает сертификаты ключей проверки электронных подписей и выдает такие сертификаты *Пользователю УЦ*, при условии установления личности *Пользователя УЦ* либо полномочия лица, выступающего от имени *Пользователя УЦ*, по обращению за получением данного сертификата;

— осуществляет в соответствии с правилами подтверждения владения ключом электронной подписи подтверждение владения *Пользователя УЦ* ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному им для получения сертификата ключа проверки электронной подписи;

— устанавливает сроки действия сертификатов ключей проверки электронных подписей;

— аннулирует выданные *Удостоверяющим центром* сертификаты ключей проверки электронных подписей;

— выдает по обращению *Пользователя УЦ* средства электронной подписи, содержащие ключ электронной подписи и ключ проверки электронной подписи (в том числе созданные удостоверяющим центром) или обеспечивающие возможность создания ключа электронной подписи и ключа проверки электронной подписи заявителем;

— ведет реестр выданных и аннулированных *Удостоверяющим центром* сертификатов ключей проверки электронных подписей, в том числе включающий в себя информацию, содержащуюся в выданных *Удостоверяющим центром* сертификатах ключей проверки электронных подписей, и информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращения или аннулирования;

— обеспечивает в установленном порядке ведение реестра сертификатов, а также обеспечивает доступ лиц к информации, содержащейся в реестре

сертификатов, в том числе с использованием информационно-телекоммуникационной сети «Интернет»;

— создает по обращениям *Пользователя УЦ* ключи электронных подписей и ключи проверки электронных подписей;

— проверяет уникальность ключей проверки электронных подписей в реестре сертификатов;

— осуществляет по обращениям участников электронного взаимодействия проверку электронных подписей;

— осуществляет иную связанную с использованием электронной подписи деятельность;

— организация взаимодействия участников системы «КриптоСвязь»{Защищенный Электронный Документооборот}.

5 Предоставление информации

5.1 Удостоверяющий центр

Удостоверяющий центр предоставляет Стороне Договора, по ее требованию:

— копию лицензии на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

— копию лицензии на право предоставления услуг передачи данных;

— копию лицензии на право предоставления услуг телематических служб;

— копию свидетельства об аккредитации удостоверяющего центра;

— копии сертификатов соответствия на используемые средства защиты информации, в т. ч. криптографические, и средства удостоверяющего центра.

5.2 Сторона Договора

Удостоверяющий центр вправе запросить, а Сторона Договора, обязана предоставить *Удостоверяющему центру* следующие документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности *Пользователя УЦ*, а также документы, подтверждающие сведения, на основании которых *Удостоверяющим центром* вносятся сведения в сертификат:

— наименование организации, адрес места регистрации, основной государственный регистрационный номер (ОГРН), идентификационный номер налогоплательщика (ИНН) и код причины постановки на налоговый учет (КПП) Стороны Договора, уполномоченным лицом которого является *Пользователь УЦ*, занимаемая должность *Пользователя УЦ;*

— нотариально заверенную копию Устава организации, нотариально заверенную копию учредительного договора (если есть);

— нотариально заверенную копию свидетельства о государственной регистрации юридического лица или свидетельства о внесении записи в ЕГРЮЛ о юридическом лице, зарегистрированном до 1 июля 2002 года / физического лица в качестве индивидуального предпринимателя, свидетельства о постановке на учет юридического лица в налоговом органе;

— выписку (нотариально заверенную копию) из Единого государственного реестра юридических лиц / Единого государственного реестра индивидуальных предпринимателей;

— копии документов о назначении уполномоченных лиц организации (в соответствии с учредительными документами организации) и/или надлежащим образом оформленные доверенности;

— сведения о наименованиях, номерах и датах выдачи документов, подтверждающих полномочия владельца квалифицированного сертификата действовать от имени юридических лиц, государственных органов, органов местного самоуправления, если информация о таких полномочиях владельца квалифицированного сертификата включена в квалифицированный сертификат;

— фамилия, имя, отчество, паспортные данные, персональный абонентский номер подвижной (мобильной) связи (*Удостоверяющий центр* не проверяет права пользования номером), адрес электронной почты (*Удостоверяющий центр* не проверяет права пользования адресом электронной почты), идентификационный номер налогоплательщика (ИНН), страховой номер индивидуального лицевого счета (СНИЛС), основной государственный регистрационный номер

индивидуального предпринимателя (ОГРНИП) (для индивидуального предпринимателя), адрес места регистрации *Пользователя УЦ;*

— иные документы, подтверждающие сведения, включаемые в сертификат в соответствии с условиями информационных систем.

Сторона Договора, обязана предоставить *Удостоверяющему центру* для направления в установленном порядке в Единую систему идентификации и аутентификации (ЕСИА) сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации.

6 Права и обязанности

6.1 Обязанности Удостоверяющего центра

— Информировать в письменной форме *Пользователя УЦ* об Условиях и порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, выдать владельцу квалифицированного сертификата Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи;

— Предоставить *Пользователю УЦ* сертификат уполномоченного лица *Удостоверяющего центра* в электронной форме;

— Использовать для создания ключа электронной подписи уполномоченного лица *Удостоверяющего центра* и формирования электронной подписи только сертифицированные в соответствии с правилами сертификации Российской Федерации средства криптографической защиты информации (средства электронной подписи);

— Строго соблюдать срок действия ключей электронной подписи *Удостоверяющего центра*, используемых для подписания изготавливаемых сертификатов, распределяя сроки их действия таким образом, чтобы по окончании таких сроков все подписанные этими ключами сертификаты прекратили свое действие;

— Использовать ключ электронной подписи уполномоченного лица *Удостоверяющего центра* только для подписи издаваемых им сертификатов Пользователей УЦ и списков отозванных сертификатов;

— Не указывать в создаваемом сертификате ключа проверки электронной подписи ключ проверки электронной подписи, который содержится в сертификате ключа проверки электронной подписи, выданном *Удостоверяющему центру* любым другим удостоверяющим центром;

— Принять меры по защите ключа электронной подписи уполномоченного лица *Удостоверяющего центра* от несанкционированного доступа;

— Организовать свою работу по UTC/GMT (Universal Time Coordinated /Greenwich Mean Time) с учетом часового пояса города Ижевска (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4). *Удостоверяющий центр* обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности;

— Обеспечить регистрацию *Пользователей УЦ* по Заявлениям о регистрации в соответствии с порядком регистрации, изложенным в настоящем Регламенте;

— Обеспечить занесение регистрационной информации *Пользователя УЦ* в Реестр *Удостоверяющего центра* и обеспечить уникальность регистрационной информации *Пользователей УЦ*, используемой для идентификации владельцев сертификатов;

— Вносить в создаваемые сертификаты только достоверную и актуальную информацию, подтвержденную соответствующими документами;

— Ознакомить под расписку *Пользователя УЦ* с информацией, содержащейся в квалифицированном сертификате;

— Обеспечивать актуальность информации, содержащейся в Реестре *Удостоверяющего центра*, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий;

— Предоставлять безвозмездно любому лицу по его обращению в соответствии с установленным порядком доступа к Реестру сертификатов информацию, содержащуюся в Реестре сертификатов, в том числе информацию об аннулировании сертификата ключа проверки электронной подписи;

— Обеспечивать круглосуточную доступность реестра *Удостоверяющего центра* в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания;

— Направлять в установленном порядке в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и

аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра);

— По желанию *Пользователя УЦ*, которому выдан квалифицированный сертификат, безвозмездно осуществить регистрацию *Пользователя УЦ* в единой системе идентификации и аутентификации;

— Обеспечивать конфиденциальность созданных *Удостоверяющим центром* ключей электронных подписей;

— Обеспечить уникальность серийных номеров изготавливаемых сертификатов *Пользователей УЦ* и уникальность ключей проверки электронной подписи в созданных сертификатах *Пользователей УЦ,* отказать *Пользователю УЦ* в создании сертификата в случае отрицательного результата проверки в реестре *Удостоверяющего центра* уникальности ключа проверки электронной подписи;

— Отказать *Пользователю УЦ* в создании сертификата в случае, если не было подтверждено то, что *Пользователь УЦ* владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному *Пользователем УЦ* для получения сертификата;

— Аннулировать (отозвать) сертификат по соответствующему Заявлению об аннулировании (отзыве) сертификата в соответствии с порядком, определенным в настоящем Регламенте;

— Аннулировать (отозвать) сертификат *Пользователя УЦ* в случае компрометации закрытого ключа уполномоченного лица *Удостоверяющего центра*, с использованием которого был издан сертификат;

— Официально уведомить об аннулировании (отзыве) сертификата всех лиц, зарегистрированных в *Удостоверяющем центре*;

— Публиковать актуальный Список отозванных сертификатов на сайтах *Удостоверяющего центра,* указанных в изданных сертификатах в расширении cRL Distribution Point, с требуемой периодичностью.

6.2 Обязанности Стороны Договора

— Известить *Удостоверяющий центр* об изменениях в документах, представленных в *Удостоверяющий центр*, и по требованию *Удостоверяющего центра* предоставить их новые редакции в течение 5-ти рабочих дней с момента регистрации изменений;

— По требованию *Удостоверяющего центра* обеспечить личную явку в *Регистрационное отделение Удостоверяющего центра* определенных представителей Стороны Договора, а также совершить иные действия, направленные на обеспечение безопасности и законности процесса получения Сертификата;

— С целью обеспечения гарантированного ознакомления Стороны Договора с полным текстом изменений и дополнений Регламента до вступления их в силу не реже одного раза в тридцать календарных дней обращаться на сайт *Удостоверяющего центра* по адресу http://infotrust.ru за сведениями об изменениях и дополнениях в Регламент.

6.3 Обязанности Пользователя УЦ

— Обеспечивать конфиденциальность ключа электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования, в частности не допускать использование принадлежащего ему ключа электронной подписи без его согласия;

— Уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

— Не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

— Использовать для создания и проверки квалифицированных электронных подписей, создания ключей квалифицированных электронных подписей и ключей

их проверки средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии законодательством Российской Федерации;

— Использовать ключ электронной подписи в соответствии с областями применения, указанными в соответствующем данному закрытому ключу сертификате (расширения Key Usage, Extended Key Usage, Application Policy и Certificate Policies сертификата);

— Не использовать ключ электронной подписи, связанный с сертификатом, заявление на аннулирование (отзыв) которого подано в *Удостоверяющий центр*, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в *Удостоверяющий центр* по момент времени официального уведомления об аннулировании (отзыве) сертификата, либо об отказе в аннулировании (отзыве);

— Не использовать ключ электронной подписи, связанный с сертификатом, который аннулирован (отозван);

— Не использовать ключ электронной подписи до предоставления *Удостоверяющему центру* подписанного сертификата, соответствующего данному ключу электронной подписи;

— Ознакомиться с информацией, содержащейся в сертификате, получить и ознакомиться с руководством по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, подтвердив этот факт предоставлением расписки в электронном или бумажном виде.

6.4 Права Удостоверяющего центра

— Запрашивать у *Пользователя УЦ* документы для подтверждения любой содержащейся в заявлениях информации;

— Запрашивать и получать у операторов базовых государственных информационных ресурсов сведения, необходимые для осуществления проверки достоверности документов и сведений, представленных *Пользователем УЦ*;

— Запрашивать и получать из государственных информационных ресурсов выписки из Единого государственного реестра юридических лиц, Единого государственного реестра индивидуальных предпринимателей и Единого государственного реестра налогоплательщиков;

— Запрашивать у *Пользователя УЦ* дополнительные, подтверждающие достоверность представленных им сведений документы в случае наличия противоречий между сведениями, представленными *Пользователем УЦ* и сведениями, полученными из государственных информационных ресурсов;

— Не принимать от *Пользователя УЦ* документы, не соответствующие требованиям действующих нормативных правовых актов Российской Федерации;

— Отказать *Пользователю УЦ* в создании сертификата в случае невыполнения *Пользователем УЦ* обязанностей, установленных Федеральным законом, принимаемыми в соответствии с ним нормативными правовыми актами, а также настоящим Регламентом;

— Отказать *Пользователю УЦ* в создании сертификата в случае, если не было подтверждено, что *Пользователь УЦ* владеет ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному *Пользователем УЦ* для получения сертификата;

— Отказать в регистрации в *Удостоверяющем центре* в случае ненадлежащего оформления необходимых регистрационных документов;

— Отказать в создании сертификата *Пользователя УЦ* в случае ненадлежащего оформления Заявления об изготовлении сертификата;

— Отказать в аннулировании (отзыве) сертификата *Пользователя УЦ* в случае ненадлежащего оформления соответствующего Заявления об аннулировании (отзыве) сертификата, а также в случае, если сертификат уже аннулирован или прекратил своё действие по другим основаниям;

— В одностороннем порядке аннулировать (отозвать) сертификат *Пользователя УЦ* с обязательным уведомлением владельца сертификата и указанием обоснованных причин;

— Без заявления *Пользователя УЦ* прекратить действие сертификата в случае в случае наличия у *Удостоверяющего центра* достоверных сведений о нарушении конфиденциальности ключа электронной подписи *Пользователя УЦ*, а также невыполнения *Пользователем УЦ* обязанностей, установленных законодательством Российской Федерации в области электронной подписи, Регламентом, а также в случае появления у *Удостоверяющего центра* достоверных сведений о том, что документы, представленные *Пользователем УЦ* в целях создания и получения им сертификата, не являются подлинными и/или не подтверждают достоверность всей информации, включённой в данный сертификат, и/или в случае, если услуга по созданию и выдаче данного сертификата не оплачена в надлежащем порядке.

6.5 Права Стороны Договора

— Обратиться в *Удостоверяющий центр* для аннулирования (отзыва) сертификата, владельцем которого является *Пользователь УЦ*, полномочия которого действовать от имени Стороны Договора, прекращены.

6.6 Права Пользователя УЦ

— Применять сертификат уполномоченного лица *Удостоверяющего центра* для проверки электронной подписи уполномоченного лица *Удостоверяющего центра* в сертификатах, созданных *Удостоверяющим центром*;

— Применять список отозванных сертификатов, созданных *Удостоверяющим центром*, для проверки статуса сертификатов, созданных *Удостоверяющим центром*;

— Применять сертификат *Пользователя УЦ* для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате;

— Для хранения личного закрытого ключа применять носитель, поддерживаемый средством электронной подписи и *Удостоверяющим центром*;

— Обратиться в *Удостоверяющий центр* с Заявлением об изготовлении сертификата;

— Обратиться в *Удостоверяющий центр* с Заявлением об аннулировании (отзыве) сертификата, владельцем которого он является, в течение срока действия соответствующего закрытого ключа;

— Обратиться в *Удостоверяющий центр* за получением информации о статусе сертификата, изданного *Удостоверяющим центром*, на определенный момент времени;

— Обратиться в *Удостоверяющий центр* за подтверждением подлинности подписи в электронном документе, сформированной с использованием сертификата, изданного *Удостоверяющим центром*.

7 Ответственность сторон

За невыполнение или ненадлежащее выполнение обязательств по настоящему Регламенту Стороны несут имущественную ответственность в пределах суммы доказанного реального ущерба, причиненного Стороне невыполнением или ненадлежащим выполнением обязательств другой Стороной. Ни одна из Сторон не отвечает за неполученные доходы (упущенную выгоду), которые бы получила другая Сторона.

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

Удостоверяющий центр не несет ответственность за неисполнение, либо ненадлежащее исполнение своих обязательств по настоящему Регламенту, а также возникшие в связи с этим убытки в случае, если *Удостоверяющий центр* обоснованно полагался на сведения, указанные в Заявлениях и других документах *Пользователя УЦ* и/или Стороны Договора.

Удостоверяющий центр несет ответственность за убытки при использовании закрытого ключа и сертификата *Пользователя УЦ* только в случае, если данные убытки возникли при компрометации ключа электронной подписи уполномоченного лица *Удостоверяющего центра*.

Удостоверяющий центр в соответствии с законодательством Российской Федерации несет ответственность за вред, причиненный третьим лицам в результате неисполнения или ненадлежащего исполнения обязательств, вытекающих из договора оказания услуг, и неисполнения или ненадлежащего исполнения обязанностей, предусмотренных Федеральным законом «Об электронной подписи».

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

Аккредитованный удостоверяющий центр (работник аккредитованного удостоверяющего центра, доверенные лица и их работники) несет гражданско-правовую, административную и (или) уголовную ответственность в соответствии с законодательством Российской Федерации за неисполнение обязанностей, установленных Федеральным законом «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, а также порядком реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей.

8 Разрешение споров

Сторонами в споре, в случае его возникновения, считаются *Удостоверяющий центр* и Сторона Договора.

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

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

Сторона, получившая от другой Стороны претензию, обязана в течение 20 (двадцати) дней удовлетворить заявленные в претензии требования или направить другой Стороне мотивированный отказ с указанием оснований отказа. К ответу должны быть приложены все необходимые документы.

Спорные вопросы между Сторонами, неурегулированные в претензионном порядке, разрешаются в Арбитражном суде Удмуртской Республики.

9 Конфиденциальность информации

9.1 Типы конфиденциальной информации

Ключ электронной подписи, соответствующий сертификату, является конфиденциальной информацией *Пользователя УЦ*. *Удостоверяющий центр* не осуществляет хранение ключей электронной подписи *Пользователей УЦ*.

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

9.2 Типы информации, не являющейся конфиденциальной

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

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

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

Информация, содержащаяся в Регламенте, не считается конфиденциальной.

9.3 Исключительные полномочия Удостоверяющего центра

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

9.4 Обработка персональных данных Пользователей УЦ

Цель обработки персональных данных *Удостоверяющим центром* — идентификация и аутентификация субъекта персональных данных в качестве

Пользователя УЦ, а также пользователя/участника информационных систем с применением электронной подписи, в которых используются сертификаты *Пользователя УЦ*.

Обработка персональных данных в *Удостоверяющем центре* осуществляется на основании согласия субъекта персональных данных — *Пользователя УЦ*. Согласие выражается путем подписания *Пользователем УЦ* установленных *Удостоверяющим центром* форм заявлений/уведомлений. Заявитель не может быть зарегистрирован в реестре *Удостоверяющего центра* без его согласия на обработку его персональных данных, в порядке и на условиях, определяемых настоящим Регламентом.

Перечень персональных данных, обрабатываемых *Удостоверяющим центром*: фамилия, имя, отчество, паспортные данные, в т.ч. адрес по месту регистрации (в случае создания сертификата физического лица), персональный абонентский номер подвижной (мобильной) связи, адрес электронной почты, идентификационный номер налогоплательщика (ИНН), страховой номер индивидуального лицевого счета (СНИЛС), основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП) и выписка из Единого государственного реестра индивидуальных предпринимателей (ЕГРИП) (для индивидуального предпринимателя) *Пользователя УЦ*. В изготавливаемые *Удостоверяющим центром* сертификаты пользователей вносятся фамилия, имя, отчество, адрес электронной почты, СНИЛС, ИНН, ОГРНИП, а также по желанию Пользователя УЦ адрес по месту регистрации (в случае создания сертификата физического лица). По требованию Организатора Системы с согласия *Пользователя УЦ* в сертификат могут быть включены дополнительные персональные данные.

Персональные данные, вносимые в сертификаты, на основании согласия *Пользователя УЦ* относятся к категории общедоступных. Обработка общедоступных персональных данных в информационных системах с применением электронной подписи может производиться *Удостоверяющим центром* и Организатором Системы с использованием средств автоматизации. Обработка

персональных данных, которые не вносятся в сертификаты, *Удостоверяющим центром* осуществляется без использования средств автоматизации.

Удостоверяющий центр осуществляет следующие действия с персональными данными: сбор, систематизацию, использование, распространение, хранение и уничтожение персональных данных.

Сбор и систематизация персональных данных *Пользователей УЦ* осуществляется в ходе приема установленных *Удостоверяющим центром* форм заявлений от лиц, проходящих процедуру регистрации/перерегистрации и создания сертификатов в соответствии с настоящим Регламентом. Сбор и систематизацию персональных данных *Пользователей УЦ* проводит *Удостоверяющий центр*, в том числе его *Регистрационные отделения*. *Регистрационное отделение* является лицом, осуществляющим обработку персональных данных по поручению оператора персональных данных. Если сбор и систематизацию персональных данных *Пользователей УЦ* проводит *Регистрационное отделение*, то оно выполняет требования, принятых *Удостоверяющим центром* организационно-распорядительных документов и действующего законодательства в области обработки и защиты персональных данных.

Полученные персональные данные используются для регистрации пользователей в реестре *Удостоверяющего центра* и для создания ключей и сертификатов путем внесения данных в соответствующие поля сертификатов.

Список должностных лиц *Удостоверяющего центра*, допущенных к обработке персональных данных *Пользователей УЦ*, утверждается организационно-распорядительным документом *Удостоверяющего центра*.

Распространение персональных данных *Пользователей УЦ Удостоверяющим центром* и/или *Пользователями УЦ* осуществляется путем передачи сертификатов по телекоммуникационным каналам связи Организатору Системы и непосредственным участникам обмена электронными документами в рамках функционирующих информационных систем с применением электронной подписи.

Персональные данные, содержащиеся в сертификатах и на бумажных носителях, подлежат обработке до принятия решения о прекращении деятельности

по оказанию услуг *Удостоверяющего центра*. Уничтожение персональных данных, содержащихся в сертификатах и на бумажных носителях, производится после принятия решения о прекращении деятельности по оказанию услуг *Удостоверяющего центра.*

Согласие на обработку персональных данных *Пользователей УЦ* может быть отозвано по письменному заявлению *Пользователя УЦ*. При этом сотрудниками *Удостоверяющего центра* производится уничтожение документов на бумажных носителях. Согласие на обработку персональных данных, содержащихся в сертификатах, не может быть отозвано и действует до принятия решения о прекращении оказания услуг *Удостоверяющим центром*.

В случае необходимости получения от *Пользователя УЦ* дополнительных персональных данных (кроме указанных в настоящем Регламенте), связанной с особыми требованиями информационной системы с электронной подписью/ Организатора Системы, указанные дополнительные персональные данные обрабатываются (собираются и хранятся) *Удостоверяющим центром* и передаются Организатору Системы только при наличии специального согласия *Пользователя УЦ* на данные действия в порядке, определенном Организатором Системы.

В соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ и разделом VI приказа Минкомсвязи России от 13.04.2012 № 107 *Удостоверяющий центр* с согласия *Пользователя УЦ* получает и направляет в установленном порядке в Единую систему идентификации и аутентификации (ЕСИА) сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, при условии соответствия этих сведений информации, содержащейся в базовых информационных ресурсах.

10 Порядок и сроки выполнения процедур (действий), необходимых для предоставления услуг Удостоверяющим центром, в том числе требования к документам, предоставляемым в Удостоверяющий центр в рамках предоставления услуг

10.1 Процедура создания ключей электронных подписей и ключей проверки электронных подписей

Пользователь УЦ может поручить сформировать ключевые документы *Удостоверяющему центру* или выполнить эту процедуру самостоятельно на своем рабочем месте с использованием средств, предоставляемых *Удостоверяющим центром*, или с использованием автоматизированного рабочего места *Удостоверяющего центра*.

При самостоятельном формировании ключей электронной подписи *Пользователь УЦ* должен соблюдать порядок использования средств криптографической защиты информации и требования по обеспечению безопасности, установленные нормативными документами органов государственного регулирования (Положение ПКЗ-2005, утвержденное приказом ФСБ России от 09.02.2005 № 66, Инструкция, утвержденная приказом ФАПСИ от 13.06.2001 № 152 и т.п.), и Руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи. Рекомендуется соблюдать требования по обеспечению безопасности информации, соответствующие законодательству Российской Федерации по технической защите конфиденциальной информации.

10.1.1 Порядок создания ключей электронных подписей и ключей проверки электронных подписей Удостоверяющим центром

Удостоверяющий центр создает ключ электронной подписи и ключ проверки электронной подписи для заявителя в соответствии с правилами пользования

средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Ключ электронной подписи и ключ проверки электронной подписи, предназначенные для создания и проверки усиленной квалифицированной электронной подписи, в соответствии с частью 4 статьи 5 Федерального закона «Об электронной подписи» создаются с использованием средства электронной подписи, имеющего подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

В этом случае *Удостоверяющим центром* обеспечивается выполнение требований, установленных постановлением Правительства Российской Федерации от 03.02.2012 № 79 в отношении автоматизированного рабочего места *Удостоверяющего центра*, используемого для создания ключа электронной подписи и ключа проверки электронной подписи для заявителя. По окончании процедуры для *Пользователя УЦ* формируются:

— ключевой носитель, содержащий ключевой контейнер ключа электронной подписи в формате, определяемом средством электронной подписи;

— сертификат *Пользователя УЦ* в электронной форме, соответствующий закрытому ключу.

Документы на электронных и бумажных носителях выдаются/направляются *Пользователю УЦ* с соблюдением требований по обеспечению конфиденциальности.

Собственноручная подпись *Пользователя УЦ* в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, Журнале учета корреспонденции по вопросам распространения средств криптографической защиты информации и ключевых документов к ним, Письме-подтверждении получения средств криптографической защиты информации и ключевых документов к ним, Акте приема-передачи и т.п. является доказательством

(подтверждением) владения *Пользователем УЦ* данным ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному в выпущенном сертификате, а также распиской в ознакомлении с информацией, содержащейся в квалифицированном сертификате, и в получении руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

10.1.2 Порядок создания ключей электронных подписей и ключей проверки электронных подписей Пользователем УЦ

Заявитель создает ключ электронной подписи и ключ проверки электронной подписи в соответствии с правилами пользования средствами криптографической защиты информации, согласованными с Федеральной службой безопасности Российской Федерации в соответствии с приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

В случае генерации ключей *Пользователем УЦ* в *Удостоверяющий центр* в электронном виде с помощью средств, предоставляемых *Удостоверяющим центром*, передается соответствующий Запрос на сертификат, формируемый в процессе генерации ключей с использованием средств, предоставляемых *Удостоверяющим центром*.

Запрос на сертификат *Пользователя УЦ* представляет собой электронный документ формата PKCS#7. В качестве подписываемых данных используется запрос на сертификат в формате PKCS#10, а электронная подпись осуществляется на закрытом ключе *Пользователя УЦ*.

Значения поля Subject в Запросе на сертификат должны быть идентичны значениям этих полей в реестре *Удостоверяющего центра*.

После получения Запроса в *Удостоверяющем центре* ответственный сотрудник *Удостоверяющего центра* проверяет соответствие Заявления и Запроса, корректность электронной подписи Запроса и устанавливает его автора, затем

сравнивает значения поля Subject содержащиеся в Запросе на сертификат, со значениями, указанными реестре *Удостоверяющего центра*.

В случае отрицательного результата проведенных проверок, а также иных случаях, установленных настоящим Регламентом, ответственный сотрудник *Удостоверяющего центра* отклоняет Запрос и уведомляет об этом *Пользователя УЦ*.

По окончании процедуры для *Пользователя УЦ* формируются:

— сертификат *Пользователя УЦ* в электронной форме, соответствующий закрытому ключу.

Указанные выше данные, передаваемые зарегистрированному *Пользователю УЦ* в электронной форме, возвращаются в виде файлов с использованием средств, предоставляемых *Удостоверяющим центром*.

10.2 Планы, основание, процедуры, сроки и порядок смены ключей электронной подписи Удостоверяющего центра

Плановая смена ключей (закрытого и соответствующего ему открытого ключа) уполномоченного лица *Удостоверяющего центра* выполняется в период действия закрытого ключа уполномоченного лица *Удостоверяющего центра* на основании максимальных сроков действия криптографических ключей, определенных эксплуатационной документацией на используемые средства электронной подписи и средства удостоверяющего центра.

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

— Уполномоченное лицо *Удостоверяющего центра* генерирует новый ключ электронной подписи и соответствующий ему ключ проверки электронной подписи;

— Уполномоченное лицо *Удостоверяющего центра* изготавливает (получает в Минкомсвязи России) новый сертификат уполномоченного лица *Удостоверяющего центра*.

Уведомление пользователей о проведении смены ключей уполномоченного лица *Удостоверяющего центра* осуществляется посредством публикации

информации на официальном сайте *Удостоверяющего центра* по адресу www.infotrust.ru с указанием доверенного способа получения нового сертификата *Удостоверяющего центра*.

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

10.3 Порядок осуществления смены ключей электронной подписи Удостоверяющего центра в случаях нарушения их конфиденциальности

В случае компрометации (или угрозы компрометации) закрытого ключа уполномоченного лица *Удостоверяющего центра* сертификат уполномоченного лица *Удостоверяющего центра* аннулируется (отзывается), Пользователи *Удостоверяющего центра* уведомляются об указанном факте путем публикации информации о компрометации на сайте *Удостоверяющего центра* www.infotrust.ru.

При использовании *Ключа электронной подписи Удостоверяющего центра* существуют угрозы нарушения конфиденциальности.

Угроза, реализованная с использованием уязвимостей информационной системы, называется атакой. Существует три основные категории атак:

— Отказ в обслуживании;

— Раскрытие информации;

— Нарушение целостности;

Для предотвращения атак на *Ключ электронной подписи Удостоверяющего центра* реализуется комплекс организационно-технических мер, при выполнении которых нарушитель не располагает программно-аппаратными средствами взаимодействия с *Удостоверяющим центром*.

Реализованные меры защиты нацелены на предотвращение компрометации или угрозы компрометации *Ключа электронной подписи Удостоверяющего центра*.

Компрометация или угроза компрометации *Ключа электронной подписи Удостоверяющего центра* является основанием полагать, что конфиденциальность *Ключа электронной подписи* нарушена.

Под компрометацией *Ключа электронной подписи* понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых *Ключ электронной подписи* может стать доступными третьим лицам и (или) процессам. К событиям, связанным с компрометацией ключей, относятся следующие:

— Потеря ключевых носителей;

— Увольнение сотрудников, имевших доступ к ключевой информации;

— Нарушение правил хранения и уничтожения (после окончания срока действия) ключа электронной подписи;

— Возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;

— Нарушение печати на сейфе с ключевыми носителями;

— Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что, данный факт произошел в результате несанкционированных действий злоумышленника).

В случае компрометации или угрозы компрометации *Ключа электронной подписи Удостоверяющего центра* выполняется внеплановая смена соответствующего ключа.

После аннулирования сертификата уполномоченного лица *Удостоверяющего центра* в срок не более 3 (трех) рабочих дней выполняется процедура внеплановой смены ключей уполномоченного лица *Удостоверяющего центра*. Процедура внеплановой смены ключей уполномоченного лица *Удостоверяющего центра*, в том числе порядок информирования владельцев сертификатов об осуществлении такой смены с указанием доверенного способа получения нового сертификата *Удостоверяющего центра*, выполняется в порядке, определенном процедурой плановой смены ключей уполномоченного лица *Удостоверяющего центра*.

Одновременно со сменой такого ключа электронной подписи прекращается действие всех квалифицированных сертификатов, созданных с использованием этого ключа электронной подписи, с занесением сведений об этих квалифицированных сертификатах в реестр квалифицированных сертификатов, и подлежат безвозмездной внеплановой смене.

10.4 Процедура создания и выдачи квалифицированных сертификатов (с регистрацией Пользователя УЦ)

Под регистрацией *Пользователей УЦ* понимается внесение регистрационной информации о пользователях *Удостоверяющего центра* в реестр *Удостоверяющего центра*. *Удостоверяющий центр* осуществляет создание сертификатов физическим лицам и уполномоченным представителям юридических лиц только в том случае, если указанное лицо является Стороной Договора.

Регистрация *Пользователя УЦ* в *Удостоверяющем центре* осуществляется на основании Заявления о регистрации при личном прибытии лица, проходящего процедуру регистрации, в офис *Удостоверяющего центра*. Форма Заявления приведена в приложениях к Регламенту: в Приложении А — для должностного лица юридического лица, в Приложении Б — для индивидуального предпринимателя или физического лица, в Приложении В — для юридического лица для автоматического создания и (или) автоматической проверки квалифицированных электронных подписей в информационной системе.

Для обеспечения юридической значимости документов на бумажных носителях, на основании которых осуществляется получение Сертификата или обеспечивается взаимодействие с Удостоверяющим центром, требуется собственноручная подпись лица и печать организации/индивидуального предпринимателя (при наличии). Подписание производится чернилами (пастой) синего цвета. Использование факсимильного воспроизведения собственноручной подписи (факсимиле, клише подписи) не допускается. Собственноручная подпись лица в представленных в *Удостоверяющий центр* документах должна соответствовать образцу его личной подписи в паспорте.

В случае если от имени юридического лица за получением квалифицированного сертификата обращается должностное лицо, не имеющее права действия без доверенности от этого юридического лица, то для подтверждения полномочий выступать от имени юридического лица и обращаться за получением квалифицированного сертификата юридического лица в *Удостоверяющий центр* у должностного лица должны быть соответствующие правомочия, указанные в Заявлении (Приложение А).

В случае если *Организатором Системы* установлены особые требования к процедурам регистрации пользователей этой системы, то к обработке принимаются Заявления о регистрации, имеющие согласительную отметку *Организатора Системы*.

Регистрация *Пользователя УЦ* в *Удостоверяющем центре* производится в течение 3 (трех) рабочих дней со дня поступления оплаты и предоставления документов, предусмотренных настоящим Регламентом, а также Запроса на сертификат (в случае формирования ключей *Пользователем УЦ* с использованием средств, предоставляемых *Удостоверяющим центром*). В случае необходимости для срочного создания и выдачи квалифицированного сертификата заявителю *Удостоверяющий центр* вправе установить отдельные условия для вознаграждения, процедура создания и выдачи квалифицированного сертификата при этом не изменяется.

Идентификация заявителя проводится при его личном присутствии.

Сотрудник *Удостоверяющего центра* выполняет процедуру идентификации лица, проходящего процедуру регистрации, путем установления личности по паспорту (в исключительных случаях отсутствия у гражданина Российской Федерации основного документа, удостоверяющего личность, *Удостоверяющий центр* может удостоверить его личность по иному документу, удостоверяющему личность, в соответствии с законодательством Российской Федерации; личность гражданина иностранного государства устанавливается по паспорту гражданина данного государства или по иному документу, удостоверяющему личность гражданина иностранного государства; личность беженца, вынужденного

переселенца и лица без гражданства удостоверяется на основании документа, установленного законодательством Российской Федерации в качестве удостоверяющего личность данных категорий лиц), проверяет корректность указания в Заявлении о регистрации Пользователя УЦ всех реквизитов (кроме адреса электронной почты), их соответствие подтверждающим документам (или их надлежащим образом заверенным копиям), а также сведениям из ЕГРЮЛ/ЕГРИП и иным источникам.

Пользователь УЦ представляет в *Удостоверяющий центр* документы (или их надлежащим образом заверенные копии), необходимые для удостоверения личности *Пользователя УЦ,* а также документы, подтверждающие сведения, на основании которых *Удостоверяющим центром* вносятся сведения в сертификат, в том числе:

— в отношении физического лица — фамилия, имя, а также отчество (при наличии), дата рождения, реквизиты документа, удостоверяющего личность, идентификационный номер налогоплательщика, страховой номер индивидуального лицевого счета гражданина в системе обязательного пенсионного страхования;

— в отношении юридического лица, зарегистрированного в соответствии с законодательством Российской Федерации, — наименование, организационно-правовая форма, идентификационный номер налогоплательщика, а также основной государственный регистрационный номер и адрес юридического лица;

— для юридического лица, зарегистрированного в соответствии с законодательством иностранного государства, — наименование, регистрационный номер, место регистрации и адрес юридического лица на территории государства, в котором оно зарегистрировано.

Если для подтверждения каких-либо сведений, вносимых в сертификат, действующим законодательством или настоящим Регламентом установлена определенная форма документа, *Пользователь УЦ* представляет в Удостоверяющий центр документ соответствующей формы. К документам, оформленным не на русском языке, должен быть приложен их официальный перевод на русский язык, заверенный нотариусом или дипломатическими (консульскими) органами.

Подтверждение достоверности сведений осуществляется одним из следующих способов:

1) с использованием оригиналов документов и (или) надлежащим образом заверенных копий документов;

2) с использованием единой системы межведомственного электронного взаимодействия, информационных систем органов государственной власти, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования, единой информационной системы нотариата;

3) с использованием единой системы идентификации и аутентификации.

Для заполнения квалифицированного сертификата *Удостоверяющий центр* запрашивает и получает из государственных информационных ресурсов необходимые сведения. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и *Удостоверяющим центром* идентифицирован заявитель, *Удостоверяющий центр* осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

В случае отказа в регистрации, Заявление о регистрации вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника *Удостоверяющего центра*.

При принятии положительного решения о регистрации, ответственный сотрудник *Удостоверяющего центра* выполняет регистрационные действия по занесению регистрационной информации в реестр *Удостоверяющего центра* и изготавливает ключи и сертификат.

Пользователь УЦ может поручить сформировать ключевые документы *Удостоверяющему центру* или выполнить эту процедуру самостоятельно на своем рабочем месте с использованием средств, предоставляемых *Удостоверяющим центром*.

Удостоверяющий центр выдает сертификаты ключей проверки электронных подписей в форме электронных документов. Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную удостоверяющим центром. По запросу Владельца сертификата сотрудник *Удостоверяющего центра* изготавливает такую копию по установленной форме (Приложение Л).

10.4.1 Идентификация Пользователя УЦ при использовании им средств, предоставляемых *Удостоверяющим центром*

При регистрации *Пользователя УЦ* в *Удостоверяющем центре*, а также при создании сертификата, в соответствующем Заявлении *Пользователь УЦ* сообщает свой персональный абонентский номер подвижной (сотовой) связи для его удаленной идентификации *Удостоверяющим центром* и получения одноразовых паролей. Форма Заявления приведена в приложениях к Регламенту: в Приложении А — для должностного лица юридического лица, в Приложении Б — для индивидуального предпринимателя или физического лица, в Приложении В — для юридического лица для автоматического создания и (или) автоматической проверки квалифицированных электронных подписей в информационной системе, в Приложении Г — для создания сертификата.

В случае изменения персонального абонентского номера подвижной (сотовой) связи *Пользователь УЦ* представляет в *Удостоверяющий центр* Заявление о замене номера телефона Пользователя Удостоверяющего центра InfoTrust, в котором сообщает актуальный персональный абонентский номера подвижной (сотовой) связи для его удаленной идентификации *Удостоверяющим центром* и получения одноразовых паролей. Форма Заявления приведена в Приложении К. При этом активный (действующий) телефонный номер может быть единственным у *Пользователя УЦ*.

При использовании средств, предоставляемых *Удостоверяющим центром, Пользователь УЦ* указывает свой персональный абонентский номер подвижной (сотовой) связи, зарегистрированный в *Удостоверяющем центре* согласно

соответствующему заявлению *Пользователя УЦ*. На указанный *Пользователем УЦ* персональный абонентский номер подвижной (сотовой) связи *Удостоверяющий центр* по сети телефонной связи в коротком текстовом сообщении (short message service, SMS) направляет одноразовый пароль (one time password, OTP — пароль, действительный в течение ограниченного промежутка времени и предназначенный только для одного сеанса аутентификации, который невозможно использовать повторно). Использование одноразовых паролей, отправляемых в коротких текстовых сообщениях (OTP via SMS) обеспечивает двухфакторную аутентификацию и предназначено для повышения уровня безопасности. Короткое текстовое сообщение с одноразовым паролем на операцию содержит также основную информацию о производимой операции.

Предъявление *Пользователем УЦ* одноразового пароля, полученного от *Удостоверяющего центра* по сети телефонной связи в коротком текстовом сообщении на зарегистрированный персональный абонентский номер подвижной (сотовой) связи *Пользователя УЦ*, с использованием средств, предоставляемых *Удостоверяющим центром,* является подтверждением удаленной идентификации и аутентификации *Пользователя УЦ* в процессе осуществления им операций с использованием средств, предоставляемых *Удостоверяющим центром.* Все действия, совершенные после удаленной идентификации и аутентификации, считаются совершенными *Пользователем УЦ*.

Предъявление *Пользователем УЦ* одноразового пароля, полученного от *Удостоверяющего центра* по сети телефонной связи в коротком текстовом сообщении на зарегистрированный персональный абонентский номер подвижной (сотовой) связи *Пользователя УЦ*, в процессе формирования ключей электронной подписи *Пользователем УЦ* с использованием средств, предоставляемых *Удостоверяющим центром,* является доказательством (подтверждением) владения *Пользователем УЦ* данным ключом электронной подписи, который соответствует ключу проверки электронной подписи, указанному в выпущенном сертификате.

В соответствии с ч. 2 ст. 160 Гражданского Кодекса Российской Федерации и ст. 11 Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об

информации, информационных технологиях и о защите информации» Стороны согласовали возможность применения *Пользователем УЦ* аналогов собственноручной подписи (АСП) для подписания электронных документов при использовании им средств, предоставляемых *Удостоверяющим центром,* а информация, подписанная АСП, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, и порождает юридические последствия.

Предъявление *Пользователем УЦ* одноразового пароля, полученного от *Удостоверяющего центра* по сети телефонной связи в коротком текстовом сообщении на зарегистрированный персональный абонентский номер подвижной (сотовой) связи *Пользователя УЦ*, в процессе формирования ключей электронной подписи *Пользователем УЦ* с использованием средств, предоставляемых *Удостоверяющим центром,* является АСП *Пользователя УЦ* — распиской в ознакомлении с информацией, содержащейся в квалифицированном сертификате, и в получении руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи.

При использовании *Пользователем УЦ* средств, предоставляемых *Удостоверяющим центром, Пользователь УЦ* должен являться пользователем услуг телефонной связи, у которого заключен договор об оказании услуг телефонной связи с оператором сотовой связи, зарегистрированным и действующим на территории Российской Федерации в порядке, предусмотренном законодательством Российской Федерации, для которого выделен уникальный абонентский номер, находиться в зоне обслуживания сети подвижной телефонной связи и иметь включенный сервис получения коротких текстовых сообщений. Направление *Удостоверяющим центром* короткого текстового сообщения *Пользователю УЦ* безвозмездно для *Пользователя УЦ*.

Пользователь УЦ обязан обеспечить защиту от несанкционированного доступа своего абонентского устройства и/или идентификационного модуля (электронный носитель информации, установленный в абонентском устройстве, с

помощью которого осуществляется идентификация абонента оператором связи, доступ абонентского устройства к сети подвижной связи, а также обеспечивается защита от несанкционированного использования абонентского номера, subscriber identity module, SIM). При утере абонентского устройства и/или идентификационного модуля *Пользователь УЦ* обязан незамедлительно сообщить в *Удостоверяющий центр*.

Срок действия и сложность одноразового пароля, содержание короткого сообщения, длительность сеанса соединения и меры по защите канала связи при использовании средств, предоставляемых *Удостоверяющим центром,* устанавливаются *Удостоверяющим центром* самостоятельно с учетом требований обеспечения безопасности информации.

Удостоверяющий центр не несет ответственности за сбои в работе сетей связи, возникшие по независящим от *Удостоверяющего центра* причинам и повлекшие за собой несвоевременное получение или неполучение *Пользователем УЦ* короткого текстового сообщения с одноразовым паролем, отсутствие у *Пользователя УЦ* доступа к средствам, с использованием которых *Пользователь УЦ* может получать короткие текстовые сообщения с одноразовым паролем.

Зарегистрированный персональный абонентский номер подвижной (сотовой) связи *Пользователя УЦ* может быть использован *Удостоверяющим центром* для идентификации *Пользователя УЦ* по телефонной связи путем сообщения *Пользователем УЦ* зарегистрированной ключевой фразой, указанной им в заявлении о регистрации *Пользователя УЦ*.

10.5 Процедура создания и выдачи квалифицированных сертификатов (без регистрации Пользователя УЦ)

Создание сертификата *Пользователя УЦ* осуществляется при плановой и внеплановой замене ключей электронной подписи *Пользователя УЦ* и производится в течение 3 (трех) рабочих дней со дня поступления оплаты и предоставления документов, предусмотренных настоящим Регламентом, а также Запроса на сертификат (в случае формирования ключей *Пользователем УЦ* с использованием

средств, предоставляемых *Удостоверяющим центром*). В случае необходимости для срочного создания и выдачи квалифицированного сертификата заявителю *Удостоверяющий центр* вправе установить отдельные условия для вознаграждения, процедура создания и выдачи квалифицированного сертификата при этом не изменяется.

Идентификация заявителя проводится при его личном присутствии или посредством идентификации заявителя без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата.

Формирование сертификата *Пользователя УЦ* осуществляется *Удостоверяющим центром* на основании Заявления об изготовлении сертификата *Пользователя УЦ,* при личном прибытии *Пользователя УЦ* в офис *Удостоверяющего центра*. Форма Заявления об изготовлении сертификата приведена в Приложении Г к *Регламенту*. Заявление может быть создано в форме электронного документа, подписанного усиленной квалифицированной электронной подписью на основе действующего квалифицированного сертификата *Пользователя УЦ*.

Если замена ключа электронной подписи владельца квалифицированного сертификата связана с нарушением его конфиденциальности или угрозой нарушения конфиденциальности, соответствующее заявление должно быть подписано иной усиленной квалифицированной электронной подписью владельца квалифицированного сертификата

В случае если *Организатором Системы* установлены особые требования к процедурам создания сертификатов пользователей этой системы, то к обработке принимаются Заявления об изготовлении сертификата, имеющие согласительную отметку *Организатора Системы*.

Сотрудник *Удостоверяющего центра* выполняет процедуру идентификации лица путем установления личности по паспорту, проверяет корректность указания в Заявлении всех реквизитов, их соответствии подтверждающим документам, а также сведениям из ЕГРЮЛ/ЕГРИП и иным источникам.

Для заполнения квалифицированного сертификата *Удостоверяющий центр* запрашивает и получает из государственных информационных ресурсов необходимые сведения. В случае если полученные из государственных информационных ресурсов сведения подтверждают достоверность информации, представленной заявителем для включения в квалифицированный сертификат, и *Удостоверяющим центром* идентифицирован заявитель, *Удостоверяющий центр* осуществляет процедуру создания и выдачи заявителю квалифицированного сертификата. В противном случае Удостоверяющий центр отказывает заявителю в выдаче квалифицированного сертификата.

В случае отказа в создании сертификата, Заявление об изготовлении сертификата вместе с приложениями возвращается заявителю с отметкой ответственного сотрудника *Удостоверяющего центра*. При принятии положительного решения *Удостоверяющий центр* изготавливает сертификат.

Пользователь УЦ может поручить сформировать ключевые документы *Удостоверяющему центру* или выполнить эту процедуру самостоятельно на своем рабочем месте с использованием средств, предоставляемых *Удостоверяющим центром*, или с использованием автоматизированного рабочего места *Удостоверяющего центра*. Генерация ключевых документов производится в порядке, установленном разделом 10.1 настоящего Регламента.

Удостоверяющий центр выдает сертификаты ключей проверки электронных подписей в форме электронных документов. Владелец сертификата ключа проверки электронной подписи, выданного в форме электронного документа, вправе получить также копию сертификата ключа проверки электронной подписи на бумажном носителе, заверенную удостоверяющим центром. По запросу Владельца сертификата сотрудник *Удостоверяющего центра* изготавливает такую копию по установленной форме (Приложение Л).

10.6 Информация о сертификатах ключей уполномоченного лица Удостоверяющего центра

Сертификаты уполномоченного лица *Удостоверяющего центра* в электронной форме распространяются *Удостоверяющим центром* через официальный сайт *Удостоверяющего центра* www.infotrust.ru, являющийся доверенным способом получения нового сертификата *Удостоверяющего центра.*

Перед установкой их на рабочие места пользователей во избежание их подмены требуется проверить подлинность устанавливаемых сертификатов по идентификатору ключа, серийному номеру и хэш-коду, опубликованному на сайте.

10.7 Компрометация ключа Пользователя УЦ

Пользователь УЦ самостоятельно принимает решение о факте или угрозе компрометации своего ключа электронной подписи.

В случае компрометации или угрозы компрометации ключа электронной подписи *Пользователь УЦ* аннулирует действие сертификата, соответствующего скомпрометированному ключу, посредством подачи Заявления об аннулировании (отзыве) сертификата.

Пользователь УЦ осуществляет внеплановую смену ключа электронной подписи и сертификата в соответствии с Регламентом.

10.8 Процедуры, осуществляемые при прекращении действия и аннулировании квалифицированного сертификата

Удостоверяющий центр аннулирует сертификат *Пользователя УЦ* в случаях, установленных статьей 14 Федерального закона «Об электронной подписи»:

— в случае прекращения действия настоящего Регламента в отношении Стороны Договора;

— в случае получения от *Пользователя УЦ* Заявления об аннулировании (отзыве) сертификата;

— в случае получения от Стороны Договора Заявления об отзыве/прекращении полномочий *Пользователя УЦ* по действию от имени Стороны Договора;

— в случае отсутствия у *Удостоверяющего центра* подтверждения, что *Пользователь УЦ* владеет ключом электронной подписи, соответствующим ключу проверки электронной подписи, указанному в таком квалифицированном сертификате;

— в случае установления *Удостоверяющим центром* факта, что содержащийся в выданном сертификате ключ проверки электронной подписи уже содержится в ином ранее созданном квалифицированном сертификате;

— в случае получения решения суда, вступившего в законную силу, если решением суда, в частности, установлено, что сертификат содержит недостоверную информацию;

— в связи с истечением установленного срока действия сертификата;

— в случае прекращения деятельности *Удостоверяющего центра* без перехода его функций другим лицам;

— при компрометации закрытого ключа уполномоченного лица *Удостоверяющего центра*.

Информация о прекращении действия сертификата вносится *Удостоверяющим центром* в *Реестр Удостоверяющего центра* в течение двенадцати часов с момента наступления указанных выше обстоятельств, связанных с необходимостью прекращения действия сертификата, или в течение двенадцати часов с момента, когда *Удостоверяющему центру* стало известно или должно было стать известно о наступлении таких обстоятельств. Действие сертификата прекращается с момента внесения записи об этом в *Реестр Удостоверяющего центра*.

Официальным уведомлением *Удостоверяющего центра* о факте отзыва сертификата является опубликование первого (наиболее раннего) списка отозванных сертификатов, содержащего сведения об отозванном сертификате, и изданного не ранее момента наступления обстоятельств, связанных с

необходимостью прекращения действия сертификата. Дата и время издания данного списка отозванных сертификатов указывается в поле thisUpdate.

Информация о местах размещения списка отозванных сертификатов заносится в изданные *Удостоверяющим центром* сертификаты в расширение cRL Distribution Point сертификата.

В случае аннулирования сертификата *Пользователя УЦ* по истечении срока его действия временем аннулирования сертификата *Пользователя УЦ* признается время, хранящееся в поле notAfter поля Validity сертификата. В данном случае информация об аннулированном сертификате *Пользователя УЦ* в список отозванных сертификатов не заносится.

В случае компрометации закрытого ключа уполномоченного лица *Удостоверяющего центра* временем аннулирования сертификата *Пользователя УЦ* признается время компрометации закрытого ключа уполномоченного лица *Удостоверяющего центра*, фиксирующееся в *Реестре Удостоверяющего центра*. В случае компрометации закрытого ключа уполномоченного лица *Удостоверяющего центра* информация о сертификате *Пользователя УЦ* в список отозванных сертификатов не заносится.

10.8.1 Аннулирование (отзыв) сертификата *Пользователя УЦ* по заявлению его владельца

Аннулирование сертификата *Пользователя УЦ* осуществляется *Удостоверяющим центром* на основании Заявления об аннулировании (отзыве) сертификата в форме документа на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью. Форма Заявления об аннулировании (отзыве) сертификата приведена в Приложении Д к *Регламенту*.

Сотрудник *Удостоверяющего центра* выполняет процедуру идентификации лица путем установления личности по документу, удостоверяющему личность, проверяет корректность указания в Заявлении всех реквизитов, их соответствии подтверждающим документам, а также сведениям из ЕГРЮЛ/ЕГРИП и иным источникам.

В случае отказа в отзыве сертификата, Заявление об аннулировании (отзыве) сертификата возвращается заявителю с отметкой ответственного сотрудника *Удостоверяющего центра*. При принятии положительного решения *Удостоверяющий центр* отзывает сертификат.

10.8.2 Аннулирование (отзыв) сертификата *Пользователя УЦ* в случае отзыва полномочий

Сторона Договора, являющаяся юридическим лицом, вправе прекратить действие Доверенностей на право действия от имени юридического лица (при их наличии) и аннулировать (отозвать) сертификаты своих полномочных представителей, зарегистрированных в *Удостоверяющем центре*, путем подачи Заявления об отзыве/прекращении полномочий *Пользователя УЦ* по действию от имени Стороны Договора в форме документа на бумажном носителе или в форме электронного документа. Форма Заявления приведена в Приложении Е к настоящему Регламенту.

После получения *Удостоверяющим центром* документа, отзывающего/прекращающего полномочия *Пользователя УЦ* по действию от имени Стороны Договора, ответственный сотрудник *Удостоверяющего центра* осуществляет его рассмотрение и обработку.

В случае отказа в отзыве сертификатов *Удостоверяющий центр* уведомляет об этом Сторону Договора. При принятии положительного решения ответственный сотрудник *Удостоверяющего центра* отзывает сертификаты *Пользователя УЦ*.

10.9 Получение информации о статусе сертификата, изданного Удостоверяющим центром

Получение информации о статусе сертификата, изданного *Удостоверяющим центром,* осуществляется на основании Заявления. Данное Заявление оформляется по форме, приведенной в Приложении Ж настоящего Регламента, и предоставляется в *Удостоверяющий центр* посредством почтовой либо курьерской связи.

Заявление должно содержать следующую информацию:

— время и дата подачи Заявления;

— время и дата, на момент наступления которых требуется установить статус сертификата;

— серийный номер сертификата, статус которого требуется установить.

По результатам проведения работ по Заявлению оформляется справка, содержащая информацию о статусе сертификата, которая предоставляется заявителю.

Предоставление справки о статусе сертификата должно быть осуществлено не позднее 10 (Десяти) рабочих дней с момента получения *Удостоверяющим центром* соответствующего Заявления.

10.10 Подтверждение действительности электронной подписи, использованной для подписания электронных документов

По желанию Стороны Договора *Удостоверяющий центр* осуществляет проведение экспертных работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов.

В том случае, если формат электронного документа с подписью соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то *Удостоверяющий центр* обеспечивает подтверждение действительности электронной подписи, использованной для подписания электронных документов. Решение о соответствии электронного документа с подписью стандарту CMS принимает *Удостоверяющий центр*.

В данном случае для подтверждения действительности электронной подписи, использованной для подписания электронных документов *Пользователь УЦ* подает Заявление в *Удостоверяющий центр* по форме, приведенной в Приложении И.

Заявление должно содержать следующую информацию:

— дата и время подачи Заявления;

— время и дата, на момент наступления которых требуется установить подлинность подписи.

Обязательным приложением к заявлению на подтверждение действительности электронной подписи, использованной для подписания электронных документов является электронный/магнитный носитель, содержащий:

— сертификат *Пользователя УЦ*, с использованием которого необходимо осуществить подтверждение подтверждению действительности электронной подписи, использованной для подписания электронных документов (в виде файла стандарта CMS);

— проверяемый электронный документ: в виде одного файла (стандарт CMS), содержащего подписанные данные и значение подписи этих данных, или двух файлов — один из которых содержит данные, а другой значение подписи этих данных (стандарт CMS).

Проведение работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов, предусматривает проверку действительности всех сертификатов, включенных в цепочку проверки до сертификата аккредитованного *Удостоверяющего центра*, выданного ему удостоверяющим центром Минкомсвязи России.

Проведение работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов, осуществляет комиссия, сформированная из числа сотрудников *Удостоверяющего центра*. Результатом проведения работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов, является заключение *Удостоверяющего центра*.

Заключение содержит:

— состав комиссии, осуществлявшей проверку;

— основание для проведения проверки;

— результат проверки подписи электронного документа;

— данные, представленные комиссии для проведения проверки.

— отчет по выполненной проверке.

Отчет по выполненной проверке содержит:

— время и место проведения проверки;

— содержание и результаты проверки;

— обоснование результатов проверки.

Заключение *Удостоверяющего центра* по выполненной проверке составляется в произвольной форме в двух экземплярах, подписывается всеми членами комиссии и заверяется печатью *Удостоверяющего центра*. Один экземпляр Заключения по выполненной проверке предоставляется заявителю.

Срок проведения работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов, и предоставлению заявителю Заключения по выполненной проверке составляет 3 (три) рабочих дня с момента поступления Заявления в *Удостоверяющий центр* при условии поступления оплаты стоимости данной услуги на расчетный счет *Удостоверяющего центра*. В том случае, если формат электронного документа с подписью не соответствует стандарту криптографических сообщений Cryptographic Message Syntax (CMS), то проведение экспертных работ по подтверждению действительности электронной подписи, использованной для подписания электронных документов, осуществляется в рамках заключения отдельного договора (соглашения) между *Удостоверяющим центром* и Стороной Договора. Перечень исходных данных для проведения экспертизы, состав и содержание отчетных документов (акты, заключения и т.д.), сроки проведения работ, размер вознаграждения Удостоверяющего центра определяются указанным договором (соглашением).

10.11 Порядок ведения реестра квалифицированных сертификатов

Формирование и ведение Реестра сертификатов осуществляется в порядке, установленном Федеральным законом «Об электронной подписи». Ведение Реестра сертификатов включает в себя:

— внесение изменений в Реестр сертификатов в случае изменения содержащихся в нем сведений;

— внесение в Реестр сертификатов сведений о прекращении действия или об аннулировании Сертификатов.

Информация, внесенная в Реестр сертификатов, подлежит хранению в течение всего срока деятельности Удостоверяющего центра, если более короткий срок не установлен законодательством Российской Федерации.

Хранение информации, содержащейся в Реестре сертификатов, осуществляется в форме, позволяющей проверить ее целостность и достоверность. Хранение в Удостоверяющем центре всех выданных Сертификатов осуществляется постоянно в форме электронных документов.

Удостоверяющий центр обеспечивает защиту информации, содержащейся в Реестре сертификатов, от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в течение всего срока своей деятельности. Формирование и ведение Реестра сертификатов осуществляется в условиях, обеспечивающих предотвращение несанкционированного доступа к нему.

Для предотвращения утраты сведений о Сертификатах, содержащихся в Реестре сертификатов, формируется его резервная копия.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре сертификатов.

Структура Реестра сертификатов формируется и ведется в соответствии с требованиями уполномоченного органа.

Срок внесения в Реестр сертификатов сведений о прекращении действия или аннулировании Сертификатов составляет не более 12 (двенадцати) часов с момента приема заявления на прекращение действия Сертификата или наступления иного события.

10.12 Порядок технического обслуживания реестра квалифицированных сертификатов

Максимальный срок планового технического обслуживания составляет 15 (Пятнадцать) часов.

Внеплановое техническое обслуживание проводится при появлении такой необходимости в оперативном режиме. Срок проведения внепланового технического обслуживания составляет 6 (шесть) часов. Срок проведения внепланового технического обслуживания может быть увеличен.

Максимальные сроки проведения планового и внепланового технического обслуживания Реестра сертификатов не может превышать установленные сроки внесения информации в Реестр сертификатов.

Удостоверяющий центр информирует участников информационного взаимодействия о проведении технического обслуживания посредством размещения информации на официальном сайте *Удостоверяющего центра*.

10.13 Предоставление Удостоверяющим центром сервиса Службы актуальных статусов сертификатов

Удостоверяющий центр оказывает услуги *Пользователям УЦ* по предоставлению актуальной информации о статусе сертификатов посредством Сервиса службы актуальных статусов сертификатов. Служба актуальных статусов сертификатов по запросам *Пользователей УЦ* формирует и предоставляет этим пользователям OCSP-ответы, которые содержат информацию о статусе запрашиваемого сертификата. OCSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов).

Служба актуальных статусов сертификатов работает по UTC/GMT (Universal Time Coordinated /Greenwich Mean Time) с учетом часового пояса города Ижевска (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4).

OCSP-ответ признается действительным при одновременном выполнении следующих условий:

— Подтверждена подлинность подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) в OCSP-ответе;

— Сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент подтверждения подлинности подписи OCSP-ответа действителен;

— Ключ электронной подписи Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) на момент формирования OCSP-ответа действителен;

— Сертификат Службы актуальных статусов сертификатов (Оператора Службы актуальных статусов сертификатов) содержит в расширении Extended Key Usage область применения — Подпись ответа службы OCSP (1.3.6.1.5.5.7.3.9);

— Сертификат *Пользователя УЦ*, статус которого установлен с использованием данного OCSP-ответа, издан *Удостоверяющим центром* и содержит в расширении Extended Key Usage или Certificate Policies область применения — Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Адрес обращения к Службе актуальных статусов сертификатов *Удостоверяющего центра* — http://z.infotrust.ru/ocsp###/ocsp.srf. Указанный адрес заносится в расширение Authority Information Access (AIA) издаваемых *Удостоверяющим центром* сертификатов, предназначенных для работы со Службой актуальных статусов сертификатов *Удостоверяющего центра*.

10.14 Предоставление Удостоверяющим центром сервиса Службы штампов времени

Удостоверяющий центр оказывает *Пользователям УЦ* услуги по выдаче штампов времени посредством сервиса Службы штампов времени. Служба штампов времени по запросам *Пользователей УЦ* формирует и предоставляет этим пользователям TSP-ответы, которые содержат информацию о текущем времени. TSP-ответы представляются в форме электронного документа, подписанного электронной подписью с использованием сертификата Службы штампов времени (Оператора Службы штампов времени).

Служба штампов времени работает по UTC/GMT (Universal Time Coordinated /Greenwich Mean Time) с учетом часового пояса города Ижевска (3-я часовая зона/МСК+1/Russia Time Zone 3) (UTC+4).

Штамп времени, относящийся к подписанному электронному документу, признается действительным при одновременном выполнении следующих условий:

— Подтверждена подлинность подписи Службы штампов времени (Оператора Службы штампов времени) в штампе времени;

— Сертификат Службы штампов времени (Оператора Службы штампов времени) на момент подтверждения подлинности подписи штампа времени действителен;

— Ключ электронной подписи Службы штампов времени (Оператора Службы штампов времени) на момент формирования штампа времени действителен;

— Сертификат Службы штампов времени (Оператора Службы штампов времени) содержит в расширении Extended Key Usage область использования — Установка штампа времени (1.3.6.1.5.5.7.3.8);

— Сертификат *Пользователя УЦ*, на котором сформирована подпись электронного документа и к которому относится данный штамп времени, издан *Удостоверяющим центром* и содержит в расширении Extended Key Usage или Certificate Policies область использования — Использование усовершенствованной электронной подписи (1.2.643.3.34.2.7).

Адрес обращения к Службе штампов времени *Удостоверяющего центра* — http://z.infotrust.ru/tsp###/tsp.srf.

Сведения о параметрах политики выдачи штампов времени указываются в штампе времени.

10.15 Предоставление Удостоверяющим центром услуг системы «КриптоСвязь»{Защищенный Электронный Документооборот}

Удостоверяющий центр оказывает *Пользователям УЦ* услуги по организации взаимодействия в системе «КриптоСвязь»{Защищенный Электронный Документооборот}.

Услуги оказываются пользователям УЦ, имеющим сертификаты, соответствующие требованиям системы.

В рамках системы обеспечивается конфиденциальность, целостность, достоверность, аутентичность и юридическая значимость электронных документов с использованием электронной подписи и шифрования файлов/почтовых сообщений.

Уровень применяемых в системе сертифицированных средств защиты информации и организационных мероприятий позволяет обмениваться электронными документами, содержащими конфиденциальную информацию (персональные данные, служебная, банковская, коммерческая тайна и т.п.).

Участники руководствуются Регламентом системы «КриптоСвязь» {Защищенный Электронный Документооборот} ООО Научно-производственное предприятие «Ижинформпроект».

11 Порядок исполнения обязанностей Удостоверяющего центра

Удостоверяющий центр производит информирование *Пользователей УЦ* об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки. Указанная информация размещается в виде Порядка использования квалифицированной электронной подписи и Руководства по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи на сайте *Удостоверяющего центра* по адресу www.infotrust.ru.

Удостоверяющий центр обеспечивает возмездную выдачу по обращению заявителя средств электронной подписи. Средства электронной подписи должны в соответствии обеспечивать возможность проверки всех усиленных квалифицированных электронных подписей в случае, если в состав электронных документов лицом, подписавшим данные электронные документы, включены электронные документы, созданные иными лицами (органами, организациями) и подписанные усиленной квалифицированной электронной подписью, или в случае, если электронный документ подписан несколькими усиленными квалифицированными электронными подписями.

Удостоверяющий центр обеспечивает актуальность информации, содержащейся в Реестре *Удостоверяющего центра*, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий путем применения организационных и технических мер, в т.ч. использования сертифицированных в установленном порядке средств защиты информации и средств удостоверяющего центра и аттестации автоматизированных систем по требованиям безопасности информации для обработки конфиденциальной информации.

Удостоверяющий центр предоставляет круглосуточный доступ к сведениям из Реестра *Удостоверяющего центра* в информационно-коммуникационной сети «Интернет», за исключением периодов планового или внепланового технического обслуживания. Максимальный срок проведения технического обслуживания — 15 (Пятнадцать) часов. О проведении планового технического обслуживания участники информационного взаимодействия уведомляются путем публикации уведомления на сайте Удостоверяющего центра за 24 (Двадцать четыре) часа до его проведения.

Удостоверяющий центр обеспечивает конфиденциальность созданных по поручению *Пользователя УЦ* ключей электронных подписей. Ключи электронных подписей, как правило, формируются непосредственно на ключевой носитель, передаваемый *Пользователю УЦ*. В случае если технология носителя/СКЗИ не позволяет сформировать ключи непосредственно на носитель или требуется создать резервный ключевой носитель, то создаваемые ключевые контейнеры временно хранятся с условием обеспечения их конфиденциальности и уничтожаются в возможно короткие сроки после их создания.

Удостоверяющий центр в порядке, установленном Федеральным законом «Об электронной подписи», направляет в единую систему идентификации и аутентификации сведения о лице, получившем квалифицированный сертификат, в объеме, необходимом для регистрации в единой системе идентификации и аутентификации, и о полученном им квалифицированном сертификате (уникальный номер квалифицированного сертификата, даты начала и окончания его действия, наименование выдавшего его аккредитованного удостоверяющего центра), а также по желанию лица, которому выдан квалифицированный сертификат, производит безвозмездную регистрацию указанного лица в единой системе идентификации и аутентификации в порядке, установленном Федеральным законом «Об электронной подписи».

Удостоверяющий центр обеспечивает предоставление безвозмездно любому лицу доступа к информации, содержащейся в реестре квалифицированных сертификатов, включая информацию о прекращении действия квалифицированного сертификата или об аннулировании квалифицированного сертификата, в том числе

путем публикации перечня прекративших свое действие (аннулированных) квалифицированных сертификатов. Сведения по каждому отдельному выданному сертификату представляются на основании отдельного запроса через форму на сайте *Удостоверяющего центра* www.infotrust.ru. Такой запрос должен содержать информацию, позволяющую идентифицировать сертификат (серийный номер сертификата), информацию об авторе запроса, адрес электронной почты для направления ответа на запрос и цель, для достижения которой должен быть представлен доступ к сертификату. Срок представления *Удостоверяющим центром* сведений — 1 (один) рабочий день. В случае получения *Удостоверяющим центром* такого запроса на бумажном носителе почтовым отправлением, срок представления Удостоверяющим центром копии сертификата на бумажном носителе составляет 7 (семь) рабочих дней.

12 Сроки действия ключевых документов

Срок действия ключа электронной подписи Уполномоченного лица *Удостоверяющего центра* составляет максимально допустимый срок действия, установленный для применяемого средства обеспечения деятельности удостоверяющего центра, и для средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи уполномоченного лица *Удостоверяющего центра* исчисляется с даты и времени генерации ключа электронной подписи уполномоченного лица *Удостоверяющего центра*.

Срок действия сертификата уполномоченного лица *Удостоверяющего центра* не превышает 18 (восемнадцать) лет. Время начала периода действия сертификата уполномоченного лица *Удостоверяющего центра* и его окончания заносится в поля «not Before» и «not After» поля «Validity Period» соответственно.

Срок действия ключей электронной подписи Службы актуальных статусов сертификатов и Службы штампов времени *Удостоверяющего центра* составляет максимально допустимый срок действия, установленный для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключей электронной подписи Службы актуальных статусов сертификатов и Службы штампов времени *Удостоверяющего центра* исчисляется с даты и времени создания сертификатов Службы актуальных статусов сертификатов и Службы штампов времени *Удостоверяющего центра*.

Срок действия сертификатов Службы актуальных статусов сертификатов и Службы штампов времени *Удостоверяющего центра* не превышает 15 (пятнадцать) лет. Время начала периода действия сертификатов Службы актуальных статусов сертификатов и Службы штампов времени *Удостоверяющего центра* и его окончания заносится в поля «not Before» и «not After» поля «Validity Period» соответственно.

Максимальный срок действия ключа электронной подписи *Пользователя УЦ* определяется максимально допустимым сроком действия, установленным для применяемого средства электронной подписи, с использованием которого данный ключ электронной подписи был сформирован.

Начало периода действия ключа электронной подписи *Пользователя УЦ* исчисляется с даты и времени начала действия соответствующего сертификата. Время начала периода действия ключа электронной подписи и его окончания может быть занесено в поле «Период использования закрытого ключа/Private Key Usage Period» сертификата.

Срок действия сертификата *Пользователя УЦ* не превышает 15 (пятнадцать) лет. Время начала периода действия сертификата *Пользователя УЦ* и его окончания заносится в поля «not Before» и «not After» поля «Validity Period» соответственно.

Типовые сроки действия сертификата *Пользователя УЦ* составляют 1 (один) год и 3 (три) года в случае использования средства электронной подписи с аппаратной компонентой ФКН (функциональный ключевой носитель).

13 Структура сертификатов и списков отозванных сертификатов

Удостоверяющий центр издает сертификаты *Пользователей УЦ* в электронной форме формата X.509 версии 3 и список отозванных сертификатов (СОС) в электронной форме формата X.509 версии 2.

Удостоверяющий центр выпускает сертификаты в соответствии с Правилами применения сертификатов, регламентирующими назначения сертификатов.

Расширения Key Usage, Extended Key Usage, Certificate Policies сертификата содержат объектные идентификаторы (OID), определяющие отношения, при осуществлении которых подписанный электронный документ, будет иметь юридическое значение.

Объектные идентификаторы, зарегистрированные в *Удостоверяющем центре* и определяющих отношения, возникающие между *Удостоверяющим центром* и Пользователями *У*Ц представлены в Перечне объектных идентификаторов ООО НПП «Ижинформпроект».

Список объектных идентификаторов, зарегистрированных в *Удостоверяющем центре* и определяющих отношения, возникающие между Пользователями УЦ — участниками конкретных информационных систем, устанавливается регламентирующими документами конкретной информационной системы.

13.1 Структура сертификата уполномоченного лица Удостоверяющего центра

Название	**Описание**	**Содержание**
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Серийный номер действующего закрытого ключа уполномоченного лица Удостоверяющего центра
Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CN = Минкомсвязь России ИНН = 007710474375 ОГРН = 1047702026701

		O = Минкомсвязь России STREET = 125375 г. Москва, ул. Тверская, д. 7 L = Москва S = 77 г. Москва C = RU E = dit@minsvyaz.ru
Validity Period	Срок действия сертификата	Действителен с: 15 сентября 2005 г. 10:22:00 UTC Действителен по: 15 сентября 2011 г. 10:28:58 UTC
Subject	Владелец сертификата	CN = ООО НПП «Ижинформпроект» OU = Удостоверяющий центр O = ООО НПП «Ижинформпроект» STREET = ул. Бородина, 21, офис 207 L = Ижевск S = 18 Удмуртская Республика C = RU E = pki@infotrust.ru
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2012) 04 40 D0 22 34 B9 C0 07 0D 56 97 02 B5 71 D5 1D 66 A8 F0 3C 8A 05 4C 2C 6E 6F C9 6C 07 1C 84 1C 59 C4 EF C0 A0 50 5A B0 A2 FA CE 2D 75 49 67 D7 8F 50 A6 A5 3E 2D 85 F8 02 99 AA DA 6C 3D 5E F3 78 D0
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость – невозможность осуществления отказа от совершенных действий, Подписывание сертификатов, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL) – сведения об отношениях, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение
Subject Key Idendifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, соответствующего данному сертификату
BasicConstraints	Основные ограничения	SubjectType (Тип владельца сертификата) = ЦС Path Length Constraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих центров)= Отсутствует
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата	Версия сертификата уполномоченного лица Удостоверяющего центра

13.2 Структура списка отозванных сертификатов

Название	Описание	Содержание
Базовые поля списка отозванных сертификатов		
Version	Версия	V2
Issuer	Издатель СОС	CN = ООО НПП «Ижинформпроект» OU = Удостоверяющий центр O = ООО НПП Ижинформпроект STREET = ул. Бородина, 21, офис 207 L = Ижевск S = 18 Удмуртская Республика C = RU E = pki@infotrust.ru
thisUpdate	Время издания СОС	дд.мм.гггг чч:мм:сс UTC
nextUpdate	Время, по которое действителен СОС	дд.мм.гггг чч:мм:сс UTC
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида 1. Серийный номер сертификата (CertificateSerialNumber) 2. Время обработки заявления на аннулирование (отзыв) и приостановление действия сертификата (Time) 3. Код причины отзыва сертификата (Reason Code) "0" Не указана "1" Компрометация ключа "2" Компрометация ЦС "3" Изменение принадлежности "4" Сертификат заменен "5" Прекращение работы "6" Приостановка действия
signatureAlgorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя СОС	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Расширения списка отозванных сертификатов		
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан СОС
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата уполномоченного лица Удостоверяющего центра

13.3 Структура сертификата Пользователя УЦ

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата

Signature Algorithm	Алгоритм подписи	ГОСТ Р 34.11/34.10-2012
Issuer	Издатель сертификата	CN = ООО НПП «Ижинформпроект» OU = Удостоверяющий центр O = ООО НПП Ижинформпроект STREET = ул. Бородина, 21, офис 207 L = Ижевск S = 18 Удмуртская Республика C = RU E = pki@infotrust.ru
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс UTC Действителен по: дд.мм.гггг чч:мм:сс UTC
Subject	Владелец сертификата	CN = Общее имя = ФИО или наименование организации SN = Фамилия G = Имя и Отчество T = Должность UN = Неструктурированное имя OU = Подразделение = наименование подразделения O = Организация = наименование организации STREET = Адрес = улица, дом, корпус L = Город = наименование населенного пункта S = Субъект РФ = Код и наименование субъекта Федерации C = Страна/Регион = RU E = Электронная почта = адрес электронной почты SNILS = СНИЛС физического лица OGRN = ОГРН организации OGRNIP = ОГРНИП индивидуального предпринимателя INN = ИНН организации/физического лица
Public Key	Открытый ключ	Открытый ключ (алгоритм ГОСТ Р 34.10-2012)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	ГОСТ Р 34.11/34.10-2012
Issuer Sign	Подпись издателя сертификата	Подпись издателя в соответствии с ГОСТ Р 34.11/34.10-2012
Дополнения сертификата		
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость - невозможность осуществления отказа от совершенных действий; Цифровая подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшеный ключ 2.5.29.37	Набор идентификаторов (OID), определяющий отношения, при осуществлении которых электронный документ с электронной подписью, сформированный с закрытым ключом, соответствующим данному сертификату, будет иметь юридическое значение
Certificate Policies	Политика сертификатов 2.5.29.32	Набор идентификаторов (OID), определяющий отношения, при осуществлении которых электронный документ с электронной подписью, сформированный с закрытым ключом, соответствующим данному сертификату, будет иметь юридическое значение
Subject Key Idendifier	Идентификатор ключа владельца сертификата	Идентификатор закрытого ключа владельца сертификата

	2.5.29.14	
Authority Key Identifier	Идентификатор ключа издателя сертификата 2.5.29.35	Идентификатор закрытого ключа уполномоченного лица Удостоверяющего центра, на котором подписан данный сертификат
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL) 2.5.29.31	http://ca.infotrust.ru/CDP/CRL_SUFFIX.crl, http://z.infotrust.ru/CDP/CRL_SUFFIX.crl, http://s.infotrust.ru/CDP/CRL_SUFFIX.crl, где CRL_SUFFIX — версия закрытого ключа уполномоченного лица Удостоверяющего центра
Authority Information Access	Адреса сертификата УЦ и Службы актуальных статусов сертификатов	URL адреса публикации сертификата уполномоченного лица Удостоверяющего центра и web-приложения Службы актуальных статусов сертификатов (заносится в сертификаты, статус которых может быть установлен по протоколу OCSP)

В сертификат могут быть добавлены дополнительные поля и расширения согласно RFC 5280.

14 Дополнительные положения

14.1 Прекращение оказания услуг Удостоверяющим центром

В случае расторжения Регламента одной из Сторон все сертификаты, владельцами которых являются *Пользователь УЦ* — Сторона Договора (если Сторона Договора — физическое лицо) и Пользователи УЦ — полномочные представители Стороны Договора (если Сторона Договора — юридическое лицо), аннулируются (отзываются) *Удостоверяющим центром*.

14.2 Хранение сертификатов в Удостоверяющем центре

Срок хранения сертификата в *Удостоверяющем центре* осуществляется в течение всего периода его действия и 5 (Пять) лет после его аннулирования (отзыва). По истечении указанного срока хранения сертификаты переводятся в режим архивного хранения. Форматы хранения сертификатов определяются эксплуатационной документацией на средства удостоверяющего центра.

14.3 Хранение документов в Удостоверяющем центре

Хранению подлежат следующие документы *Удостоверяющего центра*:

— Аннулированные сертификаты уполномоченного лица *Удостоверяющего центра* и Пользователей *УЦ*;

— Заявления о регистрации Пользователей УЦ;

— Заявления об изготовлении сертификатов;

— Заявления об аннулировании (отзыве) сертификатов;

— Служебные документы *Удостоверяющего центра.*

Документы *Удостоверяющего центра* на бумажных носителях, в том числе и сертификаты, хранятся в порядке, установленном законодательством Российской Федерации об архивах и архивном деле.

Выделение архивных документов к уничтожению и уничтожение осуществляется комиссией, формируемой из числа сотрудников УЦ.

15 Форс-мажор

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

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

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

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

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

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

Приложение А
Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ЮЛ)

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(фамилия)

_____
(имя)

_____
(отчество)

Дата рождения «___»_____ _____

Паспорт: серия □□ □□ № □□□□□□

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust

Прошу зарегистрировать меня в Удостоверяющем центре InfoTrust (УЦ) и создать на мое имя квалифицированный сертификат с профилем «Квалифицированный-ЮЛ» для информационных систем общего пользования и системы «КриптоСвязь», с расширением области применения для информационных систем _____

_____,

(наименование системы)

для использования с СКЗИ _____ класса _____.

Сообщаю персональный абонентский номер подвижной (мобильной) связи для идентификации меня Удостоверяющим центром InfoTrust и получения одноразовых паролей _____

В сертификате прошу указать следующие сведения:

Краткое наименование организации: _____

_____

ИНН ☐☐☐☐☐☐☐☐☐☐, КПП ☐☐☐☐☐☐☐☐☐,

ОГРН ☐☐☐☐☐☐☐☐☐☐☐☐☐,

Ф.И.О. (полностью): _____

СНИЛС пользователя УЦ ☐☐☐☐☐☐☐☐☐☐☐, ИНН ☐☐☐☐☐☐☐☐☐☐☐☐,

Подразделение (если есть): _____

_____

Должность: _____

_____

Населенный пункт: _____

Улица, дом, корпус/строение, помещение: _____

(по адресу местонахождения организации)

Регион РФ _____

e-mail: _____

(защита электронной почты в соответствии с S/MIME-SMTP-POP3 может быть реализована только по указанному адресу)

Определить следующую фразу (3-5 слов) _____

_____

в качестве ключевой фразы, используемой для идентификации и аутентификации Пользователя УЦ по телефону.

Варианты для указания сертифицируемого ключа проверки электронной подписи — выбрать ☑ один из представленных:

☐ Сертификат создать по Запросу, создаваемому средствами, предоставляемыми Удостоверяющим центром.

☐ Поручаю Удостоверяющему центру произвести создание ключей электронных подписей и ключей проверки электронных подписей *(требуется дополнительная оплата)*.

В соответствии со ст. 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре InfoTrust, в т.ч. его регистрационных отделениях, своих персональных данных, указанных в настоящем заявлении, а также в других документах, в целях идентификации и аутентификации меня в качестве Пользователя УЦ и информационных систем с применением электронной подписи, в т.ч. для направления в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Я согласен(на) с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом Удостоверяющего центра InfoTrust.

Я согласен(на), что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

С Регламентом Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», расположенным на сайте www.infotrust.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, опубликованных на сайте аккредитованного Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект» по адресу www.infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

К заявлению прилагаю:

— копию паспорта Пользователя УЦ (страница с ФИО и фото);

— копию страхового свидетельства обязательного пенсионного страхования Пользователя УЦ;

— копию документа о предоставлении права действия без доверенности от имени юридического лица от «___»_____ 20____ № _____;

— копию документа о назначении на должность от «___»_____ 20____ № _____.

(копии заверяются подписью уполномоченного лица и печатью организации)

Пользователь УЦ _____/_____/

Достоверность указанных сведений ПОДТВЕРЖДАЮ.

_____ предоставляет вышеуказанному регистрируемому Пользователю УЦ БЕССРОЧНО* полномочия (без права передоверия) выступать от имени юридического лица и обращаться за получением квалифицированного сертификата юридического лица в Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект» и право подписания всех необходимых документов и совершения иных действий, связанных с выполнением данного поручения.

*Действие данных полномочий может быть прекращено путем оформления и подачи Заявления об отзыве/прекращении полномочий Пользователя Удостоверяющего центра InfoTrust.

Руководитель

_____ _____/_____/
(организация)

м.п. «_____» _____ 202____

заполняется Удостоверяющим центром

Личность заявителя и его полномочия установлены. Указанные сведения проверены и соответствуют прилагаемым документам. Идентификация заявителя проведена при его личном присутствии. «_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

ООО Научно-производственное предприятие «Ижинформпроект», 426057, г. Ижевск, ул. Бородина, 21, офис 207

Приложение Б

Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ИП/ФЛ)

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(фамилия)

_____
(имя)

_____
(отчество)

Дата рождения «___»_____ _____

Паспорт: серия □□ □□ № □□□□□□

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust

Прошу зарегистрировать меня в Удостоверяющем центре InfoTrust (УЦ) и создать на мое имя квалифицированный сертификат с профилем «Квалифицированный-ИП»/«Квалифицированный-ФЛ» для информационных систем общего пользования и системы «КриптоСвязь», с расширением области применения для информационных систем _____

_____,

(наименование системы)

для использования с СКЗИ _____ класса _____.

Сообщаю персональный абонентский номер подвижной (мобильной) связи для идентификации меня Удостоверяющим центром InfoTrust и получения одноразовых паролей _____

В сертификате прошу указать следующие сведения:

ИНН □□□□□□□□□□□□,

ОГРНИП ☐☐☐☐☐☐☐☐☐☐☐☐☐, (для индивидуального предпринимателя)
Ф.И.О. (полностью): _____

СНИЛС пользователя УЦ ☐☐☐☐☐☐☐☐☐☐☐
Населенный пункт: _____
Улица, дом, корпус/строение, помещение: _____
(по адресу регистрации гражданина - ПО ЖЕЛАНИЮ)

Регион РФ _____
e-mail: _____
(защита электронной почты в соответствии с S/MIME-SMTP-POP3 может быть реализована только по указанному адресу)

Определить следующую фразу (3-5 слов) _____
_____
в качестве ключевой фразы, используемой для идентификации и аутентификации Пользователя УЦ по телефону.

Варианты для указания сертифицируемого ключа проверки электронной подписи — выбрать ☑ один из представленных:

☐ Сертификат создать по Запросу, создаваемому средствами, предоставляемыми Удостоверяющим центром.

☐ Поручаю Удостоверяющему центру произвести создание ключей электронных подписей и ключей проверки электронных подписей *(требуется дополнительная оплата)*.

В соответствии со ст. 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре InfoTrust, в т.ч. его регистрационных отделениях, своих персональных данных, указанных в настоящем заявлении, а также в других документах, в целях идентификации и аутентификации меня в качестве Пользователя УЦ и информационных систем с применением электронной подписи, в т.ч. для направления в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Я согласен(на) с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом Удостоверяющего центра InfoTrust.

Я согласен(на), что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

С Регламентом Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», расположенным на сайте www.infotrust.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях

признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, опубликованных на сайте аккредитованного Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект» по адресу www.infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

К заявлению прилагаю:
— копию паспорта Пользователя УЦ (страницы с ФИО/фото и адресом регистрации);
— копию страхового свидетельства обязательного пенсионного страхования Пользователя УЦ;

(копии заверяются подписью уполномоченного лица и печатью)

Достоверность указанных сведений ПОДТВЕРЖДАЮ.

Пользователь УЦ _____/_____/

М.П. (при наличии) «_____» _____ 202____

заполняется Удостоверяющим центром

Личность заявителя и его полномочия установлены. Указанные сведения проверены и соответствуют прилагаемым документам. Идентификация заявителя проведена при его личном присутствии. «_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

ООО Научно-производственное предприятие «Ижинформпроект», 426057, г. Ижевск, ул. Бородина, 21, офис 207

Приложение В

Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust (ИС)

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(фамилия)

_____
(имя)

_____
(отчество)

Дата рождения «___»_____ _____

Паспорт: серия ☐☐ ☐☐ № ☐☐☐☐☐☐

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление о регистрации Пользователя Удостоверяющего центра InfoTrust

Прошу зарегистрировать меня в Удостоверяющем центре InfoTrust (УЦ) и создать на мое имя квалифицированный сертификат с профилем «Квалифицированный-ИС» для информационных систем общего пользования и системы «КриптоСвязь», с расширением области применения для информационных систем _____

_____,

(наименование системы)

для использования с СКЗИ _____ класса _____.

☐Расширение области применения сертификата для аутентификации сервера

Сообщаю персональный абонентский номер подвижной (мобильной) связи для идентификации меня Удостоверяющим центром InfoTrust и получения одноразовых паролей _____

В сертификате прошу указать следующие сведения:

Краткое наименование организации: _____

_____

ИНН ☐☐☐☐☐☐☐☐☐☐, ОГРН ☐☐☐☐☐☐☐☐☐☐☐☐☐,

Населенный пункт: _____

Улица, дом, корпус/строение, помещение: _____

(по адресу местонахождения организации)

Регион РФ _____

e-mail: _____

(защита электронной почты в соответствии с S/MIME-SMTP-POP3 может быть реализована только по указанному адресу)

дополнительное поле: _____

Определить следующую фразу (3-5 слов) _____

_____

в качестве ключевой фразы, используемой для идентификации и аутентификации Пользователя УЦ по телефону.

Варианты для указания сертифицируемого ключа проверки электронной подписи — выбрать ☑ один из представленных:

☐ Сертификат создать по Запросу, создаваемому средствами, предоставляемыми Удостоверяющим центром.

☐ Поручаю Удостоверяющему центру произвести создание ключей электронных подписей и ключей проверки электронных подписей *(требуется дополнительная оплата)*.

В соответствии со ст. 9 Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» я даю согласие на обработку в Удостоверяющем центре InfoTrust, в т.ч. его регистрационных отделениях, своих персональных данных, указанных в настоящем заявлении, а также в других документах, в целях идентификации и аутентификации меня в качестве Пользователя УЦ и информационных систем с применением электронной подписи, в т.ч. для направления в Единую систему идентификации и аутентификации (ЕСИА) в соответствии с ч.5 ст.18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи». Я согласен(на) с тем, что перечень действий, общее описание способов обработки персональных данных, срок обработки, а также условия отзыва данного согласия, установлены Регламентом Удостоверяющего центра InfoTrust.

Я согласен(на), что мои персональные данные, вносимые в сертификаты, владельцем которых я буду являться, относятся к общедоступным персональным данным.

С Регламентом Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», расположенным на сайте www.infotrust.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в

квалифицированном сертификате. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, опубликованных на сайте аккредитованного Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект» по адресу www.infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

К заявлению прилагаю:

— копию паспорта Пользователя УЦ (страница с ФИО и фото);

— копию документа о предоставлении права действия без доверенности от имени юридического лица от «___»_____ 20____ № _____.

(копии заверяются подписью уполномоченного лица и печатью)

Пользователь УЦ _____/_____/

Достоверность указанных сведений ПОДТВЕРЖДАЮ.

_____ предоставляет вышеуказанному регистрируемому Пользователю УЦ БЕССРОЧНО* полномочия (без права передоверия) выступать от имени юридического лица и обращаться за получением квалифицированного сертификата юридического лица в Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект» и право подписания всех необходимых документов и совершения иных действий, связанных с выполнением данного поручения.

*Действие данных полномочий может быть прекращено путем оформления и подачи Заявления об отзыве/прекращении полномочий Пользователя Удостоверяющего центра InfoTrust.

Руководитель

_____ _____/_____/

(организация)

м.п. «_____» _____ 202____

заполняется Удостоверяющим центром

Личность заявителя и его полномочия установлены. Указанные сведения проверены и соответствуют прилагаемым документам. Идентификация заявителя проведена при его личном присутствии. «_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

ООО Научно-производственное предприятие «Ижинформпроект», 426057, г. Ижевск, ул. Бородина, 21, офис 207

Приложение Г

Заявление об изготовлении сертификата Пользователя Удостоверяющего центра InfoTrust

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(фамилия)

_____
(имя)

_____
(отчество)

Дата рождения «___»_____ _____

Паспорт: серия ☐☐ ☐☐ № ☐☐☐☐☐☐

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление об изготовлении сертификата Пользователя Удостоверяющего центра InfoTrust

В связи с плановой/внеплановой заменой ключевых документов прошу создать на мое имя квалифицированный сертификат _____

(профиль сертификата)

для информационных систем общего пользования и системы «КриптоСвязь», с расширением области применения для информационных систем _____

_____,

(наименование системы)

для использования с СКЗИ _____ класса _____.

☐Расширение области применения сертификата для аутентификации сервера.

Сообщаю персональный абонентский номер подвижной (мобильной) связи для идентификации меня Удостоверяющим центром InfoTrust и получения одноразовых паролей _____

В сертификате прошу указать сведения, предоставленные при моей регистрации в качестве Пользователя УЦ.

Варианты для указания сертифицируемого ключа проверки электронной подписи — выбрать ☑ один из представленных:

☐ Сертификат создать по Запросу, создаваемому средствами, предоставляемыми Удостоверяющим центром.

☐ Поручаю Удостоверяющему центру произвести создание ключей электронных подписей и ключей проверки электронных подписей *(требуется дополнительная оплата)*.

С Регламентом Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», расположенным на сайте www.infotrust.ru, ознакомлен(на), согласен(на), обязуюсь соблюдать.

Я ознакомился(ась) с информацией об обязанностях участников электронного взаимодействия при использовании усиленных электронных подписей и условиях признания квалифицированной электронной подписи, определенных в федеральном законе «Об электронной подписи», и обязуюсь при получении сертификата по настоящему заявлению ознакомиться с информацией, содержащейся в квалифицированном сертификате. Об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей, и о мерах, необходимых для обеспечения безопасности электронных подписей и их проверки, опубликованных на сайте аккредитованного Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект» по адресу www.infotrust.ru, проинформирован(а), руководство по обеспечению безопасности использования квалифицированной электронной подписи и средств квалифицированной электронной подписи, опубликованное на указанном сайте, получил(а).

К заявлению прилагаю:

— копию паспорта Пользователя УЦ (страницы с ФИО/фото и адресом регистрации; после обработки информации, на усмотрение Удостоверяющего центра, копия возвращается или хранится в УЦ);

— копию документа о предоставлении права действия без доверенности от имени юридического лица от «___»_____ 20____ № _____.

(копии заверяются подписью уполномоченного лица и печатью)

Пользователь УЦ _____/_____/

Достоверность указанных сведений ПОДТВЕРЖДАЮ.

Руководитель

_____ _____/_____/

м.п. «_____» _____ 202___

заполняется Удостоверяющим центром

Личность заявителя установлена. Идентификация заявителя проведена при его личном присутствии/Идентификация заявителя проведена без его личного присутствия с использованием квалифицированной электронной подписи при наличии действующего квалифицированного сертификата: № 1234567890ABCDEF.

«_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

ООО Научно-производственное предприятие «Ижинформпроект», 426057, г. Ижевск, ул. Бородина, 21, офис 207

Приложение Д

Заявление об аннулировании (отзыве) сертификата Пользователя Удостоверяющего центра InfoTrust

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(Фамилия)

_____
(Имя)

_____
(Отчество)

Дата рождения «___»_____ _____

Паспорт: серия □□ □□ № □□□□□□

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление об аннулировании (отзыве) сертификата Пользователя Удостоверяющего центра InfoTrust

В связи с _____

(причина отзыва сертификата — компрометация ключа, изменение принадлежности, прекращение работы)

прошу аннулировать (отозвать) сертификат серийный номер _____ для информационно-телекоммуникационной системы _____.

Пользователь УЦ _____/_____/

Достоверность указанных сведений ПОДТВЕРЖДАЮ.
Руководитель

_____ _____/_____/
(организация)

м.п. «_____» _____ 202___

заполняется Удостоверяющим центром

Личность заявителя установлена. Идентификация заявителя проведена при его личном присутствии. «_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

Приложение Е

Заявление об отзыве/прекращении полномочий Пользователя Удостоверяющего центра InfoTrust

_____,

(полное наименование организации с указанием организационно-правовой формы в соответствии с учредительными документами)

ИНН □□□□□□□□□□□□, КПП □□□□□□□□□,

ОГРН □□□□□□□□□□□□□□□

зарегистрированное по адресу: _____,

(место нахождения, указанное в учредительных документах)

в лице _____,

(фамилия, имя, отчество)

действующего на основании _____,

являясь Стороной Договора Удостоверяющего центра InfoTrust ООО НПП «Ижинформпроект», в связи с прекращением работы своего полномочного представителя прекращает действие Доверенностей на право действия от имени юридического лица (при их наличии) и просит аннулировать (отозвать) все действующие сертификаты, владельцем которых является зарегистрированный Пользователь УЦ InfoTrust _____.

(фамилия, имя, отчество Пользователя УЦ)

_____ _____ /_____/

(должность руководителя) (подпись) (Ф.И.О.)

«_____» _____ 202___

м.п.

заполняется Удостоверяющим центром

Личность заявителя и его полномочия установлены. Идентификация заявителя проведена при его личном присутствии. «___» _____ 202___ № _____

Представитель Удостоверяющего центра _____/_____/

Приложение Ж
Заявление о получении информации о статусе сертификата, изготовленного Удостоверяющим центром InfoTrust

_____,

(полное наименование организации с указанием организационно-правовой формы в соответствии с учредительными документами)

ИНН □□□□□□□□□□□□, КПП □□□□□□□□□,

ОГРН □□□□□□□□□□□□□□□

в лице _____,

(фамилия, имя, отчество)

действующего на основании _____,

просит предоставить информацию о статусе сертификата серийный номер _____

_____,

созданного Удостоверяющим центром InfoTrust.

Дата и время (по Ижевскому времени), на момент наступления которого требуется установить статус сертификата: «___» _____ 20___ _____часов _____ минут.

_____ _____ /_____/

(должность руководителя) (подпись) (Ф.И.О.)

«_____» _____ 202___

м.п.

заполняется Удостоверяющим центром

Документ получен «___» _____ 202___ № _____

Представитель Удостоверяющего центра _____/_____/

Приложение И
Заявление о подтверждении действительности электронной подписи, использованной для подписания электронных документов

_____,

(полное наименование организации с указанием организационно-правовой формы в соответствии с учредительными документами)

ИНН □□□□□□□□□□, КПП □□□□□□□□□, ОГРН □□□□□□□□□□□□□

в лице _____,

(фамилия, имя, отчество)

действующего на основании _____,

просит подтвердить действительность электронной подписи, использованной для подписания электронных документов, на основании следующих данных:

1. Файл в формате CMS, содержащий сертификат, с использованием которого необходимо осуществить подтверждение действительности электронной подписи в электронном документе на прилагаемом к заявлению магнитном носителе № _____;

2. Файл, содержащий подписанные данные и значение подписи в формате CMS, или файл, содержащий исходные данные, и файл, содержащий значение подписи в формате CMS, на прилагаемом к заявлению магнитном носителе № _____;

3. Дата и время (по Ижевскому времени), на момент наступления которого требуется подтвердить подлинность подписи: «___» _____ 20___ ___часов ___ минут.

_____ _____ /_____/

(должность руководителя) (подпись) (Ф.И.О.)

м.п. «_____» _____ 202___

заполняется Удостоверяющим центром

Документ получен «___» _____ 202___ № _____

Представитель Удостоверяющего центра _____/_____/

Приложение К

Заявление о замене номера телефона

Пользователя Удостоверяющего центра InfoTrust

Удостоверяющий центр InfoTrust
ООО НПП «Ижинформпроект»

_____
(Фамилия)

_____
(Имя)

_____
(Отчество)

Дата рождения «___»_____ _____

Паспорт: серия □□ □□ № □□□□□□

Дата выдачи «___»_____ 20___

Код подразделения _____-_____

Заявление о замене номера телефона
Пользователя Удостоверяющего центра InfoTrust

Сообщаю персональный абонентский номер подвижной (сотовой) связи для идентификации меня Удостоверяющим центром и получения одноразовых паролей: +7 (_____) _____-___-___ (обязательно для заполнения).

Пользователь УЦ _____/_____/

Достоверность указанных сведений ПОДТВЕРЖДАЮ.
Руководитель

_____ _____/_____/
(организация)

м.п. «_____» _____ 202___

заполняется Удостоверяющим центром

Личность заявителя установлена. Идентификация заявителя проведена при его личном присутствии.
«_____» _____ 202____ № _____

Представитель Удостоверяющего центра _____/_____/

ООО Научно-производственное предприятие «Ижинформпроект», 426057, г. Ижевск, ул. Бородина, 21, офис 207

Приложение Л

Копия сертификата на бумажном носителе

Аккредитованный Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект»
Копия квалифицированного сертификата ключа проверки электронной подписи
Сведения о сертификате:

Версия: 3
Серийный номер: 00F6CF9E152200C380E7118D29186E2029
Издатель сертификата: CN=ООО НПП «Ижинформпроект», OU=Удостоверяющий центр, O=ООО НПП «Ижинформпроект», L=Ижевск, S=18 Удмуртская Республика, C=RU, E=pki@infotrust.ru, ИНН=001831014533, ОГРН=1021801161140
Владелец сертификата: SN = Иванов, G = Иван Иванович, T = Экономист, Неструктурированное имя = 1831123456-183101001-1831123456789012, STREET = Переулок Ижевский, 3, CN = ООО "Тестовая Организация", OU = Экономический отдел, O = ООО "Тестовая Организация", L = Ижевск, S = 18 Удмуртская Республика, C = RU, E = I.Ivanov@izhevsk.ru, ИНН = 001831123456, ОГРН = 1234567890123, СНИЛС = 10987654321
Срок действия:
Действителен с: 29.12.2016 11:49:53
Действителен по: 29.12.2017 11:59:53
Ключ проверки электронной подписи:
Алгоритм: ГОСТ Р 34.11-2012/34.10-2012 256 бит (1.2.643.7.1.1.3.2)
Параметры: 30 12 06 07 2A 85 03 02 02 24 00 06 07 2A 85 03 02 02 1E 01
Значение: 04 40 D0 22 34 B9 C0 07 0D 56 97 02 B5 71 D5 1D 66 A8 F0 3C 8A 05 4C 2C 6E 6F C9 6C 07 1C 84 1C 59 C4 EF C0 A0 50 5A B0 A2 FA CE 2D 75 49 67 D7 8F 50 A6 A5 3E 2D 85 F8 02 99 AA DA 6C 3D 5E F3 78 D0

Расширения сертификата X.509

Расширение: Использование ключа (критичное)
Идентификатор: 2.5.29.15
Значение: Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных (f0)

Расширение: Улучшенный ключ
Идентификатор: 2.5.29.37
Значение: Проверка подлинности клиента (1.3.6.1.5.5.7.3.2), Защищенная электронная почта (1.3.6.1.5.5.7.3.4), Абонент Системы «Контур-Экстерн» (1.2.643.3.7.1.1.1), Защищенная информационно-телекоммуникационная система «КриптоСвязь» (1.2.643.1.10.1), Защищенное взаимодействие с Интернет-ресурсами (1.2.643.3.34.2.5), Информационная Система «Диадок» (1.2.643.3.7.3.15), Информационная Система «Контур-Экстерн» (1.2.643.3.7.1), Использование сертификата в системе межведомственного электронного документооборота государственных органов Удмуртской Республики (1.2.643.5.3.18.1), Межведомственный/межкорпоративный защищенный электронный документооборот (1.2.643.3.34.2.4), ООО НПП «Ижинформпроект» (1.3.6.1.4.1.23133), Подпись документов (соглашений, договоров, актов, писем и т.п.) (1.2.643.3.34.2.1), Пользователь Центра Регистрации, HTTP, TLS клиент (1.2.643.2.2.34.6), Представление отчетности в федеральные органы государственной власти, органы государственной власти субъектов РФ и органы местного самоуправления (1.2.643.3.34.2.2), Системы электронной коммерции (1.2.643.3.34.2.6), Участник имеющий право на включение сведений в Единый федеральный реестр сведений о фактах деятельности юридических лиц (1.2.643.3.5.10.2.12), Электронный документооборот с федеральными органами государственной власти, органами государственной власти субъектов РФ и органами местного самоуправления (1.2.643.3.34.2.3), «Квалифицированный-ЮЛ» — Квалифицированный сертификат юридического лица (1.2.643.3.34.4.1), Срок действия 12 месяцев (1.2.643.3.34.6.12)

Расширение: Идентификатор ключа центра сертификатов
Идентификатор: 2.5.29.35
Значение: Идентификатор ключа=e6 bc d0 29 36 97 29 fd b7 50 14 dc 03 80 9b 73 f6 c0 d4 63, Поставщик сертификата: Адрес каталога:CN= Минкомсвязь России, C=RU, S=77 г. Москва, L=Москва, O=Минкомсвязь России, STREET=125375 г. Москва ул. Тверская д.7, E=dit@minsvyaz.ru, ОГРН=1047702026701, ИНН=007710474375, Серийный номер сертификата=04 a8 1e 40 05 a9 18 5c 82 e6 11 13 c9 66 35 3c 81

Расширение: Идентификатор ключа субъекта
Идентификатор: 2.5.29.14
Значение: 48 23 fd e8 27 f0 04 41 c0 5d b6 df 67 be df 72 70 b2 ae 58

Расширение: Политики сертификата
Идентификатор: 2.5.29.32
Значение: [1]Политика сертификата:Идентификатор политики=Класс средства ЭП КС1, [2]Политика сертификата:Идентификатор политики=Класс средства ЭП КС2

Расширение: Период использования ключа электронной подписи
Идентификатор: 2.5.29.16
Значение: Действителен с 25 апреля 2017 г. 11:49:52 по 25 апреля 2018 г. 11:59:52

Расширение: Средства электронной подписи и УЦ издателя
Идентификатор: 1.2.643.100.112
Значение: Средство электронной подписи: "КриптоПро CSP" версия 4.0 (заключение: Сертификат соответствия № СФ/124-3010 от 30.12.2016), средство удостоверяющего центра: "КриптоПро УЦ" версии 2.0 (заключение: Сертификат соответствия № СФ/128-2983 от 18.11.2016)

Расширение: Средство электронной подписи владельца
Идентификатор: 1.2.643.100.111
Значение: Средство электронной подписи: «КриптоПро CSP» (версия 4.0)

Расширение: Точки распространения списков отзыва (CRL)
Идентификатор: 2.5.29.31
Значение: [1]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://ca.infotrust.ru/cdp/e6bcd029369729fdb75014dc03809b73f6c0d463.crl, [2]Точка распределения списка отзыва (CRL): Имя точки распространения:Полное имя:URL=http://z.infotrust.ru/cdp/e6bcd029369729fdb75014dc03809b73f6c0d463.crl
Идентификатор: 2.5.29.31

Расширение: Доступ к информации о центрах сертификации
Идентификатор: 1.3.6.1.5.5.7.1.1
Значение: [1]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://ca.infotrust.ru/infotrust-2017.crt, [2]Доступ к сведениям центра сертификации: метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2), дополнительное имя=URL=http://z.infotrust.ru/aia/infotrust-2017.crt

Подпись Удостоверяющего центра:
Алгоритм подписи: ГОСТ Р 34.11/34.10-2012 (1.2.643.7.1.1.3.2)
Параметры:
Значение: 3061 7FB3 BD46 5F59 FCC6 2A4D 7EBE A9A0 6A53 8AD8 809C 7577 1E01 AD4E 8A45 9471 B868 A5C5 76EB 3752 2131 102A CCE5 81F0 A8CD DF09 A044 B652 5A16 A02B BD09 F459

_____
Удостоверяющий центр InfoTrust ООО НПП «Ижинформпроект»
ул. Бородина, д. 21 офис 207, г. Ижевск, Удмуртская Республика, 426057
pki@infotrust.ru, www.infotrust.ru, тел/факс +7(3412) 918-100

КОПИЯ ВЕРНА
Доверенное лицо Удостоверяющего центра InfoTrust _____/_____/
«___»_____ 202____ г. м.п.

16 Лист регистрации изменений

№ п/п	Дата, №	Редакция документа	Содержание изменения
1	30.01.2012 № 5	3.2	Дополнены разделы Определения и Обозначения и сокращения. Учтены изменения, связанные с вводом в действие Постановления Правительства Российской Федерации № 725 от 31.08.2011. Дополнен подраздел Сведения об Удостоверяющем центре информацией о регистрации сертификата в Едином государственном реестре сертификатов ключей подписи уполномоченных должностных лиц удостоверяющих центров и о присоединении Удостоверяющего центра к единой системе удостоверяющих центров в области электронной цифровой подписи
2	15.08.2012 № 16	4	Внесены изменения и дополнения в связи с аккредитацией удостоверяющего центра и выпуском квалифицированных сертификатов ключей проверки электронных подписей
3	14.09.2012 № 21	4.1	Дополнен подраздел Сведения об Удостоверяющем центре информацией о регистрации сертификата в Едином государственном реестре сертификатов ключей подписи уполномоченных должностных лиц удостоверяющих центров и аккредитацией удостоверяющего центра.
4	28.05.2013 № 12	5	Изменен период публикации Списка отозванных сертификатов. Дополнен подраздел Сведения об Удостоверяющем центре информацией о регистрации сертификата в Едином государственном реестре сертификатов ключей подписи уполномоченных должностных лиц удостоверяющих центров. В соответствии с приказом ФНС России от 08.04.2013 № ММ-7-4/142@ «Об утверждении Порядка применения квалифицированных сертификатов ключей проверки электронной подписи в информационных системах ФНС России» внесены изменения в формы заявлений.
5	02.07.2013 № 14	5.1	В связи с окончанием срока действия Федерального закона от 10.01.2002 № 1-ФЗ внесены изменения в

			используемые термины по тексту документа
6	23.08.2013 № 16	5.2	Обновлены сведения о лицензиях ФСБ России и Роскомнадзора. Регламент системы «КриптоСвязь»{Защищенный Электронный Документооборот} ООО Научно-производственное предприятие «Ижинформпроект» является составной частью настоящего Регламента
7	24.10.2013 № 21	5.3	Убраны положения о процедурах приостановления/возобновления действия сертификата. Изменен порядок следования приложений. Перечень обрабатываемой информации дополнен персональным абонентским номером подвижной (мобильной) связи для идентификации удостоверяющим центром и получения одноразовых паролей.
8	14.02.2014 № 6	5.4	Изменен срок действия доверенности и порядок ее отзыва. Уточнены варианты изготовления ключей электронной подписи и ключей проверки электронной подписи.
9	29.08.2014 № 19	5.5	В связи с использованием СКЗИ с аппаратной компонентой ФКН (функциональный ключевой носитель) изменен максимальный срок действия ключа электронной подписи и внесены изменения в приложения Б, В и Ж.
10	21.10.2014 № 21	5.6	Учтены изменения, связанные с вводом в действие Федерального закона от 21.07.2014 № 248-ФЗ «О внесении изменений в Федеральный закон «Об исчислении времени».
11	19.02.2015 № 11	6.0	Порядок формирования ключевых документов Пользователя УЦ выделен в соответствующий подраздел. Дополнены разделы Определения и Обозначения и сокращения. В связи с введением публичного договора Регламент не является договором присоединения. Удалено Приложение А «Подписной лист к Регламенту». Изменен порядок следования остальных приложений.
12	16.02.2016 № 3	6.1	Учтены изменения, связанные с вводом в действие Федерального закона от 30.12.2015 № 445-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи».
13	31.08.2016 № 12	6.2	Сведения о наделении полномочиями выступать от имени юридического лица внесены в форму

			заявления (Приложение А). Удалено Приложение «Доверенность на право действия от имени юридического лица». Изменен порядок следования остальных приложений. Внесены изменения, связанные с приказом Минкомсвязи России от 08.08.2016 № 362 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей». Уточнена форма Доверенности (Приложение Г).
14	17.10.2016 № 13	6.3	Дополнены разделы 5.2 и 9.4 . Уточнены формы документов (Приложения А, Б, В, Г, Ж и Л. Обновлена информация о лицензии ФСБ России.
15	28.08.2017 № 10	6.4	Внесены изменения, связанные с приказом Минкомсвязи России от 18.11.2016 № 577 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей». Дополнены разделы 5.2 и 9.4 . Обновлена информация об аккредитации.
16	21.12.2017 № 14	6.5	Дополнены разделы 6.1 , 6.2 , 6.4 , 10.1 , 13.1 , 13.2 и 13.3 . Уточнены формы документов (Приложения А, Б).
17	29.10.2018 № 8	7	Обновлена информация о лицензиях Роскомнадзора
18	26.06.2020 № 12	8	Внесены изменения, связанные с приказом Минкомсвязи России от 13.08.2018 № 397 «Об утверждении требований к порядку реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей». Учтены изменения 63-ФЗ, вступающие в силу с 1 июля 2020, введенные Федеральным законом от 27.12.2019 № 476-ФЗ (в редакции Федерального закона от 08.06.2020 № 166-ФЗ).