Научно-производственное предприятие
“ИЖИНФОРМПРОЕКТ”

УТВЕРЖДЕН

приказом от 11.12.2017 № 13

Требования к доверенным удостоверяющим центрам системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб»)

Редакция № 1.2

КРИПТОВЕБ
ЗАЩИЩЕННЫЙ ДОКУМЕНТООБОРОТ

Ижевск 2017

Реферат

Настоящий документ содержит Требования к доверенным удостоверяющим центрам системы защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» («КриптоВеб») Общества с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект».

Требования разработаны в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Содержание

1 Определения

Система защищенного электронного юридически значимого документооборота «КриптоСвязь-Веб» (КриптоВеб) (Система) — корпоративная информационная система, устроителем которой является Организатор Системы, основанная на технологии Инфраструктуры открытых ключей (ИОК, PKI), в которой используются сертификаты, изготовленные Удостоверяющим центром, построенная на базе программных продуктов КриптоВеб, включая программное обеспечение клиентского рабочего места КриптоВеб, и предназначенная для оказания услуг в области использования электронной подписи/шифрования данных и телематических услуг связи пользователям Системы, действующая по правилам, установленным Оператором Системы в соответствии с нормативными правовыми и иными актами, регулирующими защищенный электронный документооборот и применение электронной подписи.

Оператор Системы/Оператор ЭДО — ООО НПП «Ижинформпроект», устроитель корпоративной информационной системы для обеспечения электронного документооборота с применением электронной подписи, организующий и обеспечивающий предоставление услуг пользователям Системы.

Доверенный способ передачи информации — способ передачи информации, обеспечивающий требуемую степень ее защищенности.

Сторона, присоединившаяся к Регламенту/ 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 Регламент.

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

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 — 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, выданный аккредитованным Удостоверяющим центром или доверенным

лицом аккредитованного Удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (уполномоченный федеральный орган).

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.

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), а также аккредитованные удостоверяющие центры, входящие в Перечень доверенных удостоверяющих центров *Системы* (перечень публикуется на сайте www.cryptoweb.ru).

Аккредитация удостоверяющего центра — признание уполномоченным федеральным органом соответствия удостоверяющего центра требованиям настоящего 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:

— реестр заявлений на регистрацию в Удостоверяющем центре;

— реестр зарегистрированных пользователей Удостоверяющего центра;

— реестр заявлений на изготовление 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 изготовленных 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 агентский договор, уполномоченное Удостоверяющим центром осуществлять регистрацию Пользователей УЦ и управление сертификатами Пользователей УЦ, в т.ч.:

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

— идентификация Пользователей 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.

Регламент Удостоверяющего центра (Регламент)/ Certification Practice Statement (CPS) — документ, устанавливающий общий порядок и условия предоставления Удостоверяющим центром услуг по изготовлению 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.

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.

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

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 (Регламент Удостоверяющего центра)
CRL	Certificate Revocation List (Список отозванных сертификатов)
DN	Distinguished Name (Отличительное имя)
OID	Object IDentifier (Объектный идентификатор)
OCSP	Online Certificate Status Protocol (Протокол установления актуального статуса сертификата)
PKI	Public Key Infrastructure (Инфраструктура Открытых Ключей)
RFC	Request For Comments
TLS	Transport Layer Security Protocol (Протокол криптографической защиты на транспортном уровне)
TSP	Time-Stamp Protocol (Протокол получения штампа времени)
URL	Uniform Resource Locator (Единый локатор ресурса)
UTC/GMT	Universal Time Coordinated/Greenwich Mean Time (Универсальное координированное время/Всемирное время «по Гринвичу»)
КСКПЭП	Квалифицированный сертификат ключа проверки электронной подписи (Квалифицированный сертификат)
КС	Квалифицированный сертификат (Квалифицированный сертификат ключа проверки электронной подписи)
КЭП	Квалифицированная электронная подпись
ПО	Программное обеспечение
СОС	Список отозванных сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЭДО	Электронный документооборот

3 Введение

3.1 Сведения об Операторе

Общество с ограниченной ответственностью научно-производственное предприятие «Ижинформпроект» (ООО НПП «Ижинформпроект»), предоставляющее услуги *Оператора Системы* в соответствии с требованиями законодательства Российской Федерации, именуемое в дельнейшем «*Оператор*», зарегистрировано на территории Российской Федерации в городе Ижевске.

Оператор 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 18.08.2013 № 111185;

3) лицензия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) на оказание телематических услуг связи от 18.08.2013 № 111186.

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

Контактная информация

телефон/факс: +7 (3412) 918-100,

e-mail: info@cryptoweb.ru

www: www.cryptoweb.ru

3.2 Идентификация документа

Наименование документа — Требования к доверенным удостоверяющим центрам системы защищенного юридически значимого электронного документооборота «КриптоСвязь-Веб» («КриптоВеб»).

Версия: 1.2.

Дата: 11.12.2017.

Количество страниц в документе: 35.

3.3 Статус документа

Требования к доверенным удостоверяющим центрам системы защищенного юридически значимого электронного документооборота «КриптоСвязь-Веб» («КриптоВеб») (далее — Требования) разработаны в соответствии с действующим законодательством Российской Федерации и определяют требования к квалифицированным сертификатам ключей проверки электронной подписи и аккредитованным удостоверяющим центрам и принципы взаимодействия аккредитованных удостоверяющих центров, входящих в перечень доверенных удостоверяющих центров *Системы* защищенного юридически значимого электронного документооборота.

Любые справки по вопросам, связанным с предоставлением услуг *Оператора*, предоставляются сотрудниками *Оператора* по телефону +7 (3412) 918-100 и info@cryptoweb.ru.

3.4 Применение документа

Стороны понимают термины, применяемые в настоящем документе, строго в контексте общего смысла документа.

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 документу с положениями собственно документа, Стороны считают доминирующим смысл и формулировки документа.

3.5 Изменения (дополнения) документа

Внесение изменений (дополнений) в Требования, включая приложения к ним, производится *Оператором* в одностороннем порядке.

Уведомление доверенных удостоверяющих центров *Системы* о внесении изменений (дополнений) в Требования осуществляется *Оператором* путем

направления указанных изменений (дополнений) *Оператором* на адрес электронной почты доверенного удостоверяющего центра.

Все изменения (дополнения), вносимые *Оператором* в Требования и не связанные с изменением действующего законодательства Российской Федерации, вступают в силу и становятся обязательными для доверенных удостоверяющих центров по истечении 30 (тридцати) календарных дней с момента направления *Оператором* указанных изменений и дополнений в Требования.

Все изменения (дополнения), вносимые *Оператором* в Требования 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 Требования с момента вступления в силу равно распространяются на все доверенные удостоверяющие центры *Системы*.

4 Доверенный удостоверяющий центр

Доверенный удостоверяющий центр *Системы* должен выполнять функции, предусмотренные ст. 13 и ст. 15 Федерального закона Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Доверенный удостоверяющий центр *Системы* должен иметь:

1) Лицензию Федеральной службы безопасности Российской Федерации на осуществление деятельности 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) по следующим видам выполняемых работ и оказываемых услуг: Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств; Работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); Передача шифровальных (криптографических) средств; Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

2) Свидетельство об аккредитации удостоверяющего центра в соответствии с Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Указанные документы не должны быть отозванными, их действие не должно быть приостановлено или прекращено в течение всего срока действия статуса доверенного удостоверяющего центра *Системы*.

Ключи электронной подписи и ключи проверки электронной подписи (далее — криптографические ключи) должны изготавливаться доверенным удостоверяющим центром с условием обеспечения конфиденциальности ключей электронной подписи по поручению владельца квалифицированного сертификата или самостоятельно владельцем с использованием средств, предоставляемых доверенным удостоверяющим центром.

Доверенный удостоверяющий центр должен использовать в своей деятельности сертифицированное средство удостоверяющего центра по классу не ниже КС2. При формировании криптографических ключей удостоверяющим центром и квалифицированных сертификатов должно использоваться сертифицированное средство криптографической защиты информации по классу не ниже КС2. Сертификаты соответствия на используемые средства криптографической защиты информации и средства удостоверяющего центра должны быть действительны в течение всего срока действия статуса доверенного удостоверяющего центра.

Автоматизированная система доверенного удостоверяющего центра, содержащая программно-аппаратный комплекс средств обеспечения деятельности, должна обеспечивать обработку конфиденциальной информации и соответствовать установленным требованиям нормативной документации по безопасности информации по классу не ниже 1Г. Аттестат соответствия должен быть действителен в течение всего срока действия статуса доверенного удостоверяющего центра.

Период выпуска доверенным удостоверяющим центром списка отозванных сертификатов должен быть не более 24 часов. При этом интервал перекрытия между

моментом публикации и сроком действительности должен быть не более 4 часов. Доступ к публикуемым спискам отозванных сертификатов должен обеспечиваться по различным каналам связи (публикация списков отозванных сертификатов на двух и более www-серверах, доступных через разные Интернет-провайдеры). Информация о точках публикации списка отозванных сертификатов доверенного удостоверяющего центра должна включаться в изготавливаемые квалифицированные сертификаты.

5 Средства криптографической защиты информации

Для использования в Системе доверенный удостоверяющий центр должен изготавливать *Абонентам Системы* квалифицированные сертификаты на основе средства шифрования и электронной подписи, применяемого для создания и проверки электронной подписи, средство криптографической защиты информации «КриптоПро CSP». Применяемые версии указанных средств криптографической защиты информации должны соответствовать требованиям, установленным в соответствии с Федеральным законом от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».

Для обеспечения аутентификации и защиты канала передачи данных по протоколу TLS, шифрования электронных документов и применения электронных подписей в формате CMS применяются:

— алгоритм зашифрования/расшифрования данных и вычисление имитовставки в соответствии с ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая»;

— алгоритм формирования и проверки электронной подписи в соответствии с ГОСТ Р 34.10-2001. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм формирования и проверки цифровой подписи в соответствии с ГОСТ Р 34.10-2012. «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи»;

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования»,

— алгоритм выработки значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования»,

с использованием RFC 4357, RFC 4490 и RFC 4491.

Максимальные сроки действия криптографических ключей и квалифицированных сертификатов доверенного удостоверяющего центра и *Абонентов Системы* должны удовлетворять требованиям эксплуатационной документации на применяемые сертифицированные в установленном порядке средства криптографической защиты информации и средства удостоверяющего центра.

6 Квалифицированные сертификаты

Абоненты Системы используют, принимают и признают квалифицированные сертификаты ключей проверки электронной подписи, созданные Аккредитованным Удостоверяющим центром InfoTrust ООО НПП «Ижинформпроект» и аккредитованными удостоверяющими центрами, входящими в Перечень доверенных удостоверяющих центров *Системы*.

Для получения в *Удостоверяющем центре* квалифицированного сертификата *Абонент Системы* обращается в *Удостоверяющий центр* в порядке, определенном Регламентом *Удостоверяющего центра*.

Квалифицированные сертификаты должны соответствовать требованиям:

— Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

— Приказа ФСБ РФ от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»;

— раздела Структура сертификата настоящего документа.

7 Структура сертификата

Удостоверяющий центр должен издавать квалифицированные сертификаты пользователей УЦ и уполномоченного лица *Удостоверяющего Центра* в электронной форме формата X.509 версии 3 (RFC 5280).

7.1 Объектные идентификаторы алгоритма

Удостоверяющий центр может использовать следующие идентификаторы алгоритмов средств шифрования и электронной подписи (RFC 4491, RFC 4357 и технического комитета по стандартизации «Криптографическая защита информации» (ТК 26)):

Наименование	*OID*
ГОСТ Р 34.11-94 (функция хеширования)	1.2.643.2.2.9
ГОСТ Р 34.10-2001 (электронная подпись)	1.2.643.2.2.19
ГОСТ 28147-89 (шифрование)	1.2.643.2.2.21
Диффи-Хеллмана (согласование ключа)	1.2.643.2.2.98
Диффи-Хеллмана (согласование ключа)	1.2.643.2.2.99
алгоритм подписи ГОСТ Р 34.10-2012 с ключом 256	1.2.643.7.1.1.1.1
алгоритм подписи ГОСТ Р 34.10-2012 с ключом 512	1.2.643.7.1.1.1.2
алгоритм хэширования ГОСТ Р 34.11-2012 с длиной 256	1.2.643.7.1.1.2.2
алгоритм хэширования ГОСТ Р 34.11-2012 с длиной 512	1.2.643.7.1.1.2.3
алгоритм подписи ГОСТ Р 34.10-2012 с ключом 256 с хэшированием ГОСТ Р 34.11-2012	1.2.643.7.1.1.3.2
алгоритм подписи ГОСТ Р 34.10-2012 с ключом 512 с хэшированием ГОСТ Р 34.11-2012	1.2.643.7.1.1.3.3
алгоритм HMAC на основе ГОСТ Р 34.11-2012 с ключом 256 со значениями B = 64, L = 32	1.2.643.7.1.1.4.1
алгоритм HMAC на основе ГОСТ Р 34.11-2012 с ключом 512 со значениями B = 64, L = 64	1.2.643.7.1.1.4.2
алгоритмы согласования ключа на основе ГОСТ Р 34.10-2012 для ключа 256	1.2.643.7.1.1.6.1
алгоритмы согласования ключа на основе ГОСТ Р 34.10-2012 для ключа 512	1.2.643.7.1.1.6.2

7.2 Формы имени

В сертификате поля идентификационных данных уполномоченного лица *Удостоверяющего центра* и владельца сертификата содержат атрибуты имени

формата X.500 (Distinguished Name), отличного от имен всех остальных пользователей.

7.3 Атрибуты идентификационных данных

Атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, и представляющим юридическое лицо, являются:

Наименование	*Описание*
Common Name	Полное или сокращенное наименование организации (обязательное)
Surname	Фамилия должностного лица (обязательное)
Given Name	Имя и отчество должностного лица (обязательное)
Title	Должность (обязательное)
Unstructured Name	ИНН организации-КПП организации-ИНН владельца сертификата
Organization	Полное или сокращенное наименование организации (обязательное)
Organization Unit	Наименование подразделения организации (если имеется)
Street Address	Наименование улицы, номера дома, а также корпуса, строения, квартиры, помещения по адресу местонахождения организации (обязательное)
Locality	Наименование населенного пункта по адресу местонахождения организации (обязательное)
State	Код и наименование Субъекта РФ по адресу местонахождения организации (обязательное)
Country	RU (обязательное)
Email	Адрес электронной почты
OGRN	ОГРН организации (обязательное)
SNILS	СНИЛС должностного лица (обязательное)
INN	ИНН организации (обязательное)

Атрибутами поля идентификационных данных владельца сертификата, являющегося индивидуальным предпринимателем, являются:

Наименование	*Описание*
Common Name	Фамилия, имя, отчество индивидуального предпринимателя (обязательное)
Surname	Фамилия индивидуального предпринимателя (обязательное)
Given Name	Имя и отчество индивидуального предпринимателя (обязательное)
Unstructured Name	ИНН индивидуального предпринимателя — XXXX00000 (где XXXX – код налогового органа) — ИНН индивидуального

	предпринимателя
Street Address	Наименование улицы, номера дома, а также корпуса, строения, квартиры, помещения по адресу регистрации индивидуального предпринимателя (по желанию)
Locality	Наименование населенного пункта по адресу регистрации индивидуального предпринимателя (обязательное)
State	Код и наименование Субъекта РФ по адресу регистрации индивидуального предпринимателя (обязательное)
Country	RU (обязательное)
Email	Адрес электронной почты
OGRNIP	ОГРНИП индивидуального предпринимателя (обязательное)
SNILS	СНИЛС индивидуального предпринимателя (обязательное)
INN	ИНН индивидуального предпринимателя (обязательное)

Атрибутами поля идентификационных данных владельца сертификата, являющегося физическим лицом, являются:

Наименование	*Описание*
Common Name	Фамилия, имя, отчество (обязательное)
Surname	Фамилия (обязательное)
Given Name	Имя и отчество (обязательное)
Street Address	Наименование улицы, номера дома, а также корпуса, строения, квартиры, помещения по адресу регистрации (по желанию)
Locality	Наименование населенного пункта по адресу регистрации (обязательное)
State	Код и наименование Субъекта РФ по адресу регистрации (обязательное)
Country	RU (обязательное)
Email	Адрес электронной почты
SNILS	СНИЛС (обязательное)
INN	ИНН (обязательное)

По согласованию с *Оператором Системы* возможно использование в квалифицированных сертификатах *Абонентов Системы* иных атрибутов поля идентификационных данных владельца сертификата.

7.4 Сферы применения сертификата

Сферы применения сертификата, указываемые в полях Extended Key Usage (EKU) и Certificate Policies (CP):

OID	*Описание*	*Расширение*	*Примечание*
1.3.6.1.5.5.7.3.2	Проверка подлинности клиента	EKU	Технологический

Удостоверяющий центр может на свое усмотрение указывать в квалифицированных сертификатах, используемых в *Системе*, объектные идентификаторы согласно требованиям иных информационных систем в соответствии с соглашениями с владельцами указанных объектных идентификаторов.

Использование объектных идентификаторов ООО НПП «Ижинформпроект» в сертификатах и информационных системах без письменного разрешения ООО НПП «Ижинформпроект» не допускается.

Запрещено изготавливать для *Абонентов Системы* квалифицированные сертификаты, содержащие ограничения по работе и подписанию документов в *Системе*.

8 Статус доверенного удостоверяющего центра

Статус доверенного удостоверяющего центра *Системы* предоставляется, приостанавливается и аннулируется *Оператором Системы*. Информация о статусе публикуется в Перечне доверенных удостоверяющих центров Системы на сайте *Оператора Системы* www.cryptoweb.ru.

8.1 Получение статуса

Удостоверяющий центр-претендент направляет *Оператору Системы* заявление о включении в Перечень доверенных удостоверяющих центров, содержащее реквизиты организации (полное и краткое наименование, ИНН, КПП, ОГРН, юридический и фактический адрес, наименование, БИК, ИНН банка, р/с, к/с), сведения о соответствии настоящим требованиям и копии подтверждающих документов, заверенные удостоверяющим центром-претендентом:

— Лицензия Федеральной службы безопасности Российской Федерации на осуществление деятельности 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);

— Свидетельство об аккредитации удостоверяющего центра в соответствии с Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

— Аттестат соответствия автоматизированной системы, содержащей программно-аппаратный комплекс средств обеспечения деятельности требованиям нормативной документации по безопасности информации;

— Тестовые ключи электронной подписи и тестовый квалифицированный сертификат Абонента Системы;

— Квалифицированные сертификаты удостоверяющего центра и соответствующие им квалифицированные сертификаты удостоверяющего центра, изготовленные Головным удостоверяющим центром Министерства связи и массовых коммуникаций Российской Федерации;

— Адреса публикации квалифицированных сертификатов удостоверяющего центра в сети Интернет;

— Адрес публикации регламента удостоверяющего центра в сети Интернет;

— Адреса публикации списков отозванных сертификатов удостоверяющего центра в сети Интернет с указанием используемых провайдеров услуг Интернет;

— Адрес места нахождения, адрес официального сайта в сети Интернет, адрес электронной почты, телефон и факс удостоверяющего центра, а также пунктов/точек регистрации, соответствующих установленным требованиям.

Оператор Системы в течение 15 рабочих дней рассматривает заявление, прилагаемые копии документов, производит тестирование технологической совместимости квалифицированных сертификатов для работы в *Системе* и принимает решение о включении удостоверяющего центра в Перечень доверенных удостоверяющих центров *Системы*. При положительном решении *Оператор Системы* заключает с Удостоверяющим центром-претендентом соглашение. Информация в Перечне публикуется *Оператор Системы* после оформления указанного соглашения.

Оператор Системы оставляет за собой право отказать удостоверяющему центру-претенденту во включении его в Перечень доверенных удостоверяющих центров *Системы* без объяснения причин.

8.2 Приостановление и аннулирование статуса

В случае нарушения *Удостоверяющим центром* настоящих требований, а также условий соглашения с *Оператором Системы*, *Оператор Системы* на срок до 90 календарных дней приостанавливает статус доверенного удостоверяющего центра и за 3 рабочих дня до момента приостановления уведомляет об этом *Удостоверяющий центр* и *Абонентов Системы*.

Удостоверяющий центр в течение периода приостановления статуса не имеет права изготавливать квалифицированные сертификаты *Абонентам Системы.*

Если в течение периода приостановления статуса *Удостоверяющий центр* не исправит нарушения, то *Оператор Системы* имеет право аннулировать статус доверенного удостоверяющего центра.

Удостоверяющий центр вправе приостановить или аннулировать статус по своей инициативе, направив *Оператору Системы* письменное заявление за тридцать дней до предполагаемой даты приостановления/аннулирования статуса.

9 Обязанности

9.1 Обязанности Оператора Системы

Выполнять требования нормативных документов органов исполнительной власти при обеспечении обмена информацией по телекоммуникационным каналам связи в рамках электронного документооборота, в отношении которого такие требования установлены.

Обеспечить функционирование программно-аппаратного комплекса Системы в соответствии с требованиями эксплуатационной документации на него.

Осуществлять техническую поддержку программных средств *Абонентов Системы*.

9.2 Обязанности Удостоверяющего центра

Выполнять функции, предусмотренные Федеральным законом Российской Федерации от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Выполнять требования нормативных документов органов исполнительной власти при осуществлении функций удостоверяющего центра.

Использовать сертифицированные средства криптографической защиты информации и средства удостоверяющего центра в соответствии с требованиями, определенными эксплуатационной документацией.

Принимать меры для предотвращения несанкционированного доступа к средствам удостоверяющего центра с установленными на них средствами криптографической информации, а также в помещения, в которых они установлены. Своевременно проводить оценку соответствия автоматизированной системы, содержащей программно-аппаратный комплекс средств обеспечения деятельности, установленным требованиям нормативной документации по безопасности информации для обработки конфиденциальной информации.

Своевременно публиковать списки отозванных сертификатов и обеспечивать к ним круглосуточный доступ по различным каналам связи (публикация списков

отозванных сертификатов на двух и более www-серверах, доступных через разные Интернет-провайдеры).

Оказывать *Абонентам Системы* техническую поддержку по использованию квалифицированных сертификатов, изготовленных *Удостоверяющим центром*.

Немедленно известить *Оператора Системы* об изменениях в документах и сведениях, представленных *Оператору*.

Немедленно информировать *Оператора Системы* о факте компрометации ключей электронной подписи и прекратить использование ключей электронной подписи в случае их компрометации.

10 Ответственность сторон

За невыполнение или ненадлежащее выполнение обязательств 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, а также возникшие в связи с этим убытки в случаях, если это является следствием встречного неисполнения либо ненадлежащего встречного исполнения другой Стороной своих обязательств.

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

11 Разрешение споров

При рассмотрении спорных вопросов, связанных с настоящим документом, 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) рабочих 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.

12 Вознаграждение Оператора Системы, сроки и порядок расчетов

12.1 Вознаграждение Оператора Системы

Вознаграждение *Оператора Системы* устанавливается в соответствии с соглашением между *Оператором Системы* и *Удостоверяющим центром*.

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

12.2 Сроки и порядок расчетов

Сроки и порядок расчетов устанавливается в соответствии с соглашением между *Оператором Системы* и *Удостоверяющим центром*.

13 Конфиденциальность информации

Под конфиденциальной информацией подразумевается любая информация и данные, представляющие собой коммерческую, служебную или иную тайну и персональные данные, доступ к которым ограничивается в соответствии с законодательством Российской Федерации, а также любая иная информация, помеченная как конфиденциальная или в письменном виде явно определенная в качестве таковой.

Оператор или *Удостоверяющий центр*, получившие конфиденциальную информацию, обязаны использовать ее исключительно в целях эксплуатации *Системы*, охранять ее конфиденциальность и, если иное прямо не установлено законом, не раскрывать эту информацию, как полностью, так и частично, третьим лицам, за исключением работников или контрагентов, которым эта информация необходима для выполнения возложенных на них обязательств.

К конфиденциальной информации не относится информация, которая: была известна стороне, получившей информацию, до ее предоставления; самостоятельно созданная этой Стороной до такого предоставления; стала общеизвестной не по причине действий или бездействия стороны, получившей информацию.

Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

Персональные данные, содержащиеся в сертификатах *Пользователей УЦ*, на основании согласия *Пользователя УЦ* относятся к категории общедоступных. В сведениях об учетных записях пользователей *Абонентов Системы*, доступных *Абонентам Системы*, могут быть использованы только общедоступные персональные данные, полученные из сертификатов Пользователей УЦ.

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

14 Форс-мажор

Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств при эксплуатации *Системы*, если это неисполнение явилось следствием форс-мажорных обстоятельств.

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, 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 отодвигается соразмерно времени, в течение которого действуют такие обстоятельства.

Сторона, для которой создалась невозможность исполнения своих обязательств, 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.

Неизвещение 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 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 тогда ни одна из Сторон не вправе требовать возмещения возникших у нее убытков другой Стороной.

15 Лист регистрации изменений

№ п/п	*Дата, №*	*Редакция документа*	*Содержание изменения*
1	17.11.2016 № 17	1.1	Переоформлена лицензия ФСБ России
2	11.12.2017 № 13	1.2	Обновлен раздел 7.3