РЕГЛАМЕНТ

Удостоверяющего Центра

СЗАО «Интерднестрком»

Версия 2.0

2024г.

ОГЛАВЛЕНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Бизнес-система **–** обобщенное понятие корпоративной информационной системы, эксплуатирующейся в СЗАО «Интерднестрком» (далее - Компания), в которой используются ключи электронной подписи, сертификаты открытых ключей электронной подписи, предоставляющей услуги Пользователям – участникам данной системы.

Владелец сертификата открытого ключа электронной подписи (Владелец сертификата) - лицо, которому Удостоверяющим центром выдан Сертификат открытого ключа, и которое владеет соответствующим закрытым ключом, позволяющим с помощью средств электронной подписи создавать свою Электронную подпись в Электронных документах (подписывать Электронные документы).

От имени юридического лица Владельцем сертификата открытого ключа электронной подписи может выступать:

− руководитель организации, т.е. лицо, имеющее право действовать от имени юридического лица без доверенности;

− сотрудник организации, действующий от имени юридического лица на основании доверенности (уполномоченный представитель Заявителя – юридического лица).

Заявитель − юридическое лицо независимо от организационно-правовой формы, физическое лицо (в том числе лицо, зарегистрированное в качестве индивидуального предпринимателя, частный нотариус, адвокат), обращающиеся в Удостоверяющий центр для получения Сертификата***, обладающее полной дееспособностью.***

После создания Сертификата Заявитель становится Владельцем сертификата - Пользователем УЦ.

Закрытый ключ электронной подписи (закрытый ключ) – уникальная последовательность символов, сформированная средствами электронной подписи и предназначенная для создания электронной подписи.

Закрытый ключ действует на определенный момент времени если:

− наступил момент времени начала действия закрытого ключа;

− срок действия закрытого ключа не истек;

− сертификат открытого ключа электронной подписи, соответствующий данному закрытому ключу электронной подписи, не аннулирован.

Компрометация закрытого ключа – нарушение конфиденциальности закрытого ключа.

Область действия сертификата открытого ключа электронной подписи – включенные в сертификат открытого ключа электронной подписи сведения об отношениях, при которых электронный документ с электронной подписью, созданной с использованием соответствующего сертификата открытого ключа электронной подписи, будет иметь юридическое значение.

Обработка заявления на аннулирование сертификата открытого ключа электронной подписи – совокупность действий по занесению сведений об аннулировании сертификата открытого ключа электронной подписи в реестр сертификатов Удостоверяющего Центра и уведомлению Владельца сертификата об аннулировании сертификата.

Открытый ключ электронной подписи (открытый ключ) – уникальная последовательность символов, сформированная средствами электронной подписи, однозначно связанная с закрытым ключом и предназначенная для проверки подлинности электронной подписи.

Пользователь Удостоверяющего центра (Пользователь УЦ) – лицо, присоединившееся к Регламенту, зарегистрированное в УЦ.

Правовой статус Владельца Сертификата – специальное обозначение в документах и запросах, оформляемых на основании настоящего Регламента, физических лиц, на имя которых выдается Специальный Сертификат:

– Нотариус (notary);
– Частный нотариус (private notary);
– Судебный исполнитель (marshal);
– Следователь, дознаватель (coroner);
– Налоговый инспектор (taxer).

Рабочий день Удостоверяющего Центра (далее – рабочий день) – промежуток времени с 09:00 до 18:00 каждого дня недели за исключением выходных и праздничных дней. Выходные и праздничные дни определяются с учетом переносов дней на основании решений Правительства ПМР.

Рассмотрение заявления на аннулирование действия сертификата открытого ключа электронной подписи – принятие Оператором Удостоверяющего центра решения об обработке

заявления на аннулирование сертификата открытого ключа электронной подписи на основе предоставленных документов.

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

- реестр заявлений о присоединении к Регламенту Удостоверяющего Центра;
- реестр зарегистрированных Пользователей Удостоверяющего Центра;
- реестр запросов на сертификат открытого ключа электронной подписи;
- реестр заявлений на аннулирование сертификата открытого ключа электронной подписи;
- реестр сертификатов открытых ключей электронной подписи;
- реестр изготовленных списков отозванных сертификатов;
- реестр отозванных (аннулированных) сертификатов открытого ключа электронной подписи.

Сертификат открытого ключа электронной подписи (Сертификат) − электронный документ, содержащий открытый ключ, подписанный электронной подписью Удостоверяющего Центра и подтверждающий принадлежность открытого ключа владельцу сертификата открытого ключа электронной подписи, а также позволяющий идентифицировать данного владельца.

Секретное слово – комбинация букв, цифр, символов в количестве не менее шести, сгенерированная Пользователем УЦ при формировании запроса на создание Сертификата открытого ключа электронной подписи.

Специальный Сертификат открытого ключа электронной подписи (Специальный Сертификат) – Сертификат открытого ключа электронной подписи специального назначения, который выдается Удостоверяющим Центром Пользователю для подтверждения подлинности электронной подписи и идентификации Владельца Сертификата открытого ключа электронной подписи, у которого есть полномочия для подписания запросов в электронной форме, направляемых в СЗАО «Интеднестрком» для получения информации, составляющей тайну электросвязи в соответствии с действующим законодательством ПМР. Все условия, указанные в Регламенте в отношении Сертификата, распространяются на Специальный Сертификат в части не противоречащей сути Специального Сертификата.

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.

Средства электронной подписи – программные и (или) технические средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка подлинности электронной подписи, создание закрытого и открытого ключей электронной подписи.

Стороны Регламента − Компания и Пользователь Удостоверяющего центра Компании.

Тарифы – внутренний документ Компании, устанавливающий размер вознаграждения за оказываемые услуги Пользователям УЦ.

Токен − устройство в виде USB-флеш-накопителя с защищенной паролем картой памяти, являющееся носителем ключей, на котором хранится необходимая информация для создания электронной подписи.

Удостоверяющий Центр Компании (Удостоверяющий Центр, УЦ) − функциональное подразделение Компании, выполняющее следующие основные функции:

- изготавливает сертификаты открытых ключей электронной подписи;
- с письменного согласия владельца сертификата открытого ключа электронной подписи создает ключи электронных подписей с обеспечением технической невозможности копирования закрытого ключа электронной подписи;
- аннулирует сертификаты открытых ключей электронной подписи;
- ведет реестр Удостоверяющего Центра, обеспечивает его актуальность;
- проверяет уникальность ключей электронной подписи;
- выдает сертификаты открытых ключей электронной подписи с информацией об их действии;
- осуществляет подтверждение подлинности электронной подписи в электронном документе;
- осуществляет иные функции, предусмотренные действующим законодательством ПМР.

Уполномоченное лицо Удостоверяющего Центра (Оператор УЦ) – работник Компании, действующий в соответствии с внутренними документами Компании от имени УЦ.

Электронный документ – информация, представленная в электронной форме, пригодная для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронная подпись (ЭП) − информация в электронной форме, которая присоединена или иным образом связана с другой информацией в электронной форме и которая используется для определения лица, подписывающего информацию.

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

PKCS#7 – стандарт, определяющий формат и синтаксис криптографических сообщений. Удостоверяющий центр использует описанный в PKCS#7 тип данных PKCS#7 signed – подписанные данные. Электронный документ, оформленный с соблюдением требований PKCS#7 signed, является электронным документом, содержащим электронную подпись;

PKCS#10 – стандарт, определяющий формат и синтаксис запроса на сертификат открытого ключа электронной подписи. Электронный документ, оформленный с соблюдением требований PKCS#10, содержит информацию о сертифицируемом ключе проверки электронной подписи, используемом криптографическом средстве и данные, необходимые для идентификации владельца сертифицируемого открытого ключа электронной подписи.

Internet Assigned Numbers Authority (IANA, ассоциация IANA) – международная организация, координирующая выделение объектных идентификаторов, предназначенных для идентификации телекоммуникационных объектов.

XAdES – XML Advanced Electronic Signatures (XAdES). Набор форматов усовершенствованной подписи документов XML. Спецификация размещена в электронной форме по адресу http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Предмет Регламента

2.1.1. Настоящий Регламент Удостоверяющего Центра Компании (далее - Регламент) определяет условия предоставления и правила пользования услугами Удостоверяющего Центра, включая права, обязанности, ответственность Удостоверяющего Центра и Пользователей Удостоверяющего Центра, форматы данных, основные организационно-технические мероприятия, направленные на обеспечение работы Удостоверяющего Центра.

2.1.2. Настоящий Регламент является договором присоединения в соответствии со статьей 445 Гражданского кодекса Приднестровской Молдавской Республики (далее - ПМР).

2.2. Действие Регламента

2.2.1. С момента регистрации Заявления о присоединении к настоящему Регламенту в Удостоверяющем центре лицо, подавшее Заявление, считается присоединившемся к Регламенту, и является Стороной Регламента.

2.2.2. Удостоверяющий центр вправе отказать любому лицу в приёме и регистрации Заявления о присоединении к Регламенту Удостоверяющего центра Компании в случае нарушения / ненадлежащего исполнения требований настоящего Регламента, в том числе при оформлении и передачи документации.

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

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

2.2.5. Положения Регламента УЦ, касающиеся условий и процедур изготовления, выдачи, замены, отзыва, компрометации, аннулирования сертификатов открытых ключей электронной подписи, являются более приоритетными по отношению к аналогичным положениям иных документов, регламентирующих взаимоотношения и Стороны, присоединившейся к Регламенту.

2.2.6. Настоящий Регламент опубликован в электронной форме на сайте УЦ, по адресу – http://ca.idc.md/documents.

2.2.7. Внесение изменений (дополнений) в Регламент, включая приложения к нему, производится УЦ в одностороннем порядке.

2.2.8. Уведомление о внесении изменений или дополнений в Регламент и уточненная редакция Регламента публикуются в электронной форме на сайте УЦ, по адресу – http://ca.idc.md/documents.

2.2.9. Все изменения (дополнения), вносимые УЦ в Регламент по собственной инициативе, и не связанные с изменением действующего законодательства вступают в силу и становятся обязательными по истечении 10 рабочих дней даты публикации новой редакции Регламента на сайте УЦ, по адресу – http://ca.idc.md/documents.

2.2.10. Все изменения (дополнения), вносимые УЦ в Регламент в связи с изменением действующего законодательства вступают в силу одновременно с вступлением в силу изменений (дополнений) в соответствующих нормативных актах.

2.2.11. Любые изменения и дополнения в Регламенте с момента вступления в силу равно распространяются на всех лиц, присоединившихся к Регламенту, в том числе присоединившихся к Регламенту ранее даты вступления изменений (дополнений) в силу.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Права Удостоверяющего Центра

Удостоверяющий Центр имеет право**:**

3.1.1. Аннулировать сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра в случае установленного факта компрометации соответствующего ключа электронной подписи, с уведомлением владельца аннулированного сертификата открытого ключа электронной подписи.

3.1.2. Отказать в изготовлении сертификата открытого ключа электронной подписи Пользователя в случае, если для формирования запроса на сертификат открытого ключа электронной подписи используется средство электронной подписи, не являющееся средством УЦ.

3.1.3. Пользоваться иными правами, предусмотренными действующим законодательством ПМР и настоящим Регламентом.

3.2. Права Пользователя Удостоверяющего Центра

Пользователь УЦ имеет право:

3.2.1. Получить сертификат открытого ключа электронной подписи УЦ в порядке, предусмотренном настоящим Регламентом.

3.2.2. Получить список аннулированных (отозванных) сертификатов, изготовленный УЦ.

3.2.3. Применять сертификат открытого ключа электронной подписи УЦ для проверки электронной подписи УЦ в сертификатах, изготовленных УЦ.

3.2.4. Применять сертификат открытого ключа электронной подписи Пользователя УЦ для проверки электронной подписи электронных документов в соответствии со сведениями, указанными в сертификате открытого ключа электронной подписи.

3.2.5. Применять список аннулированных (отозванных) сертификатов, изготовленный УЦ, для проверки статуса сертификатов открытых ключей электронной подписи.

3.2.6. Обратиться в УЦ за подтверждением подлинности электронных подписей в электронных документах.

3.2.7. Обратиться в УЦ за подтверждением подлинности электронных подписей УЦ в изготовленных им сертификатах открытых ключей электронной подписи.

3.2.8. Сформировать ключ электронной подписи месте своего нахождения (место нахождения персонального компьютера или иного устройства) с использованием средства электронной подписи, предоставленного УЦ.

3.2.9. Для хранения закрытого ключа электронной подписи использовать Токен, предоставленный Удостоверяющим центром, либо иной носитель (средство криптографической защиты информации).

3.2.10. Воспользоваться предоставляемыми УЦ программными средствами для формирования запроса в УЦ на создание и выдачу сертификата открытого ключа электронной подписи в электронном виде.

3.2.11. Воспользоваться предоставляемыми УЦ программными средствами, чтобы получить и установить изготовленный УЦ сертификат открытого ключа электронной подписи в электронном виде на Токен, предоставленный УЦ.

3.2.12. Обратиться в УЦ для аннулирования (отзыва) сертификата открытого ключа электронной подписи в течение срока действия соответствующего ключа электронной подписи.

3.2.13. Обратиться в УЦ за получением нового сертификата открытого ключа электронной подписи в течение срока действия Сертификата (при плановой смене открытого ключа ЭП Пользователя УЦ).

3.2.14. Обратиться в Удостоверяющий центр за получением Токена для хранения открытого и закрытого ключа и сертификата открытого ключа.

3.3. **Обязанности Удостоверяющего Центра**

Удостоверяющий Центр обязан:

3.3.1. Использовать закрытый ключ электронной подписи УЦ только для подписи издаваемых им сертификатов открытых ключей электронной подписи Пользователей УЦ и списков аннулированных сертификатов.

3.3.2. Принять меры по защите ключа электронной подписи УЦ от несанкционированного доступа.

3.3.3. Организовать свою работу по GMT (Greenwich Mean Time) с учетом часового пояса города Тирасполь. УЦ обязан синхронизировать по времени все свои программные и технические средства обеспечения деятельности.

3.3.4. Обеспечить регистрацию Пользователей УЦ в соответствии с порядком регистрации, изложенным в настоящем Регламенте. УЦ обязан обеспечить проверку идентичности лица, которому выдается сертификат открытого ключа и уникальность регистрационной информации Пользователей УЦ, используемой для идентификации владельцев сертификатов открытых ключей электронной подписи.

3.3.5. Изготовить сертификат открытого ключа электронной подписи зарегистрированного Пользователя в соответствии с порядком, определенным в настоящем Регламенте.

3.3.6. Обеспечить уникальность серийных номеров изготавливаемых сертификатов открытых ключей электронной подписи Пользователей УЦ.

3.3.7. Обеспечить уникальность значений открытых ключей электронной подписи в изготовленных сертификатах открытых ключей электронной подписи Пользователей УЦ.

3.3.8. Аннулировать сертификат открытого ключа электронной подписи по заявлению на аннулирование сертификата открытого ключа электронной подписи, не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление, внести сведения об аннулированном сертификате в список аннулированных сертификатов с указанием даты и времени занесения и причины аннулирования.

3.3.9. Вести реестр Удостоверяющего Центра.

3.3.10. Отказать в аннулировании сертификата открытого ключа электронной подписи Пользователя УЦ в случае, если истек установленный срок действия ключа электронной подписи, соответствующего этому сертификату.

3.3.11. Информировать в письменной форме заявителей об условиях и о порядке использования электронных подписей и средств электронной подписи, о рисках, связанных с использованием электронных подписей и средств электронной подписи, и о мерах, необходимых для обеспечения безопасности электронных подписей и средств их проверки.

3.3.12. Обеспечивать актуальность информации, содержащейся в реестре сертификатов, и ее защиту от неправомерного доступа, уничтожения, модификации, блокирования, иных неправомерных действий в соответствии с требованиями Закона ПМР «Об электронном документе и электронной подписи».

3.3.13. 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 открытого ключа.

3.3.14. При выдаче сертификатов открытых ключей проверять достоверность данных, указанных в заявлении на сертификацию открытого ключа, на основании документов, подтверждающих указанные данные.

3.3.15. Вносить информацию в реестр сертификатов о выдаваемом сертификате открытого ключа не позднее указанной в нем даты начала действия такого сертификата.

3.3.16. Обеспечивать соответствие информации, содержащейся в сертификате открытого ключа, информации, представленной владельцем сертификата открытого ключа;

3.3.17. Уведомлять владельца сертификата открытого ключа о ставших известными УЦ фактах, указывающих на невозможность дальнейшего использования закрытого ключа, а также об аннулировании сертификата открытого ключа.

3.3.18. Исполнять иные обязанности, предусмотренные действующим законодательством ПМР и настоящим Регламентом.

3.4. **Обязанности Пользователя Удостоверяющего Центра**

Пользователь Удостоверяющего центра обязан:

3.4.1. Хранить в тайне закрытый ключ электронной подписи, принимать все возможные меры для предотвращения его потери, раскрытия, искажения и несанкционированного использования, обеспечивать необходимые условия для исключения доступа другого лица к своему закрытому ключу.

3.4.2. Не применять закрытый ключ электронной подписи, если Пользователю стало известно, что этот ключ использовался ранее другими лицами, используется или возможно будет использоваться другими лицами (при имеющихся основаниях полагать, что нарушена конфиденциальность закрытого ключа).

3.4.3. Применять закрытый ключ электронной подписи только в соответствии с областями действия, указанными в соответствующем данному ключу электронной подписи сертификате открытого ключа электронной подписи, если такие области действия установлены.

3.4.4. Незамедлительно требовать приостановления действия или отзыва сертификата открытого ключа в случае:

3.4.4.1. потери закрытого ключа электронной подписи;

3.4.4.2. наличия оснований полагать, что нарушена конфиденциальность закрытого ключа;

3.4.4.3. несоответствия действительности информации, содержащейся в сертификате открытого ключа;

3.4.4.4. если Владелец Специального Сертификата утратил по каким-либо причинам свои полномочия на подписание запросов в электронной форме для получения информации, составляющей тайну электросвязи в соответствии с действующим законодательством ПМР.

3.4.5. Не использовать закрытый ключ электронной подписи, связанный с сертификатом открытого ключа электронной подписи, заявление на аннулирование и приостановление которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование сертификата в УЦ по момент времени официального уведомления Пользователя об аннулировании сертификата.

3.4.6. Уведомлять в течение 24 (двадцати четырех) часов удостоверяющий центр о любых изменениях сведений, содержащихся в сертификате открытого ключа.

3.4.7. Не использовать закрытый ключ электронной подписи, связанный с сертификатом открытого ключа электронной подписи, который аннулирован.

3.4.8. Регулярно, но не реже одного раза в 10 дней, просматривать сайт УЦ, по адресу http://ca.idc.md/documents на предмет изменения Регламента.

3.4.9. Ежедневно просматривать изменения в реестре аннулированных (отозванных) сертификатов открытого ключа электронной подписи на сайте УЦ, по адресу https://ca.idc.md/certificates/revoked.

3.4.10. Оплачивать вознаграждение за услуги, оказываемые Удостоверяющим Центром, в соответствии с Тарифами.

3.4.11. Исполнять иные обязанности, предусмотренные действующим законодательством ПМР и настоящим Регламентом.

4. ПРАВИЛА ПОЛЬЗОВАНИЯ УСЛУГАМИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

4.1. Регистрация Пользователей

Порядок регистрации Пользователей в Удостоверяющем Центре изложен в настоящем Регламенте и приложениях к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

4.2. Генерация ключей

Порядок генерации ключей электронной подписи Пользователей Удостоверяющего Центра изложен в приложениях к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

4.3. Изготовление и получение сертификата открытого ключа электронной подписи

Порядок изготовления и получения сертификатов открытого ключа электронной подписи Пользователей Удостоверяющего Центра изложен в настоящем Регламенте и приложениях к данному Регламенту, которые описывают процедуры регистрации Пользователей, генерации ключей, управления сертификатами открытого ключа электронной подписи.

4.4. Аннулирование сертификата открытого ключа электронной подписи

4.4.1. Удостоверяющий Центр аннулирует сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра в следующих случаях:

− по заявлению Пользователя Удостоверяющего Центра;
− по истечении срока его действия;
− при компрометации ключа электронной подписи уполномоченного лица Удостоверяющего Центра;
− при обнаружении недостоверности сведений, указанных в Заявлении на создание и выдачу сертификата открытого ключа электронной подписи или в сертификате открытого ключа;
− в связи со смертью или потерей дееспособности владельца сертификата открытого ключа, в связи с ликвидацией юридического лица, выданного такому юридическому лицу;
− по решению суда, вступившему в законную силу, в частности, если решением суда установлено, что сертификат открытого ключа содержит недостоверную информацию;
− в иных случаях, установленных действующим законодательством ПМР или настоящим Регламентом.

4.4.2. В случае компрометации ключа электронной подписи Удостоверяющего Центра временем аннулирования сертификата Пользователя Удостоверяющего Центра признается время компрометации ключа электронной подписи Удостоверяющего Центра, фиксирующееся в реестре Удостоверяющего Центра. В случае компрометации ключа электронной подписи Удостоверяющего Центра информация о сертификате Пользователя Удостоверяющего Центра в список аннулированных сертификатов не заносится.

4.4.3. Аннулирование сертификата открытого ключа электронной подписи по заявлению Пользователя (отзыв Сертификата):

Для осуществления аннулирования сертификата открытого ключа электронной подписи Пользователь подает Заявление на аннулирование сертификата открытого ключа электронной подписи в Удостоверяющий центр, составленное по форме, указанной в приложениях к Регламенту.

Аннулирование сертификата открытого ключа электронной подписи Пользователя УЦ осуществляется УЦ на основании заявления:

- в бумажной форме в соответствии с Приложением к настоящему Регламенту, опубликованным на сайте УЦ http://ca.idc.md/documents, поданного в УЦ. Рассмотрение заявления на аннулирование сертификата, оформленного в бумажном виде, осуществляется в течение рабочего дня;
- в электронной форме, в порядке, предусмотренном в Инструкции по работе с программой «IDC: Управление ключами», опубликованной на сайте УЦ, по адресу http://ca.idc.md/documents с использованием секретного слова, которое Пользователь УЦ вводил при генерации запроса на выдачу данного сертификата.

4.4.4. В случае аннулирования сертификата по заявлению Пользователя УЦ должен официально уведомить Пользователя и всех лиц, зарегистрированных в УЦ, об аннулировании сертификата не позднее одного рабочего дня с момента подачи заявления в УЦ путем размещения соответствующей информации в реестре аннулированных сертификатов открытого ключа электронной подписи, опубликованном на сайте УЦ, по адресу http://ca.idc.md/certificates .

4.4.5. Информация о размещении списка отозванных сертификатов заносится в изданные Удостоверяющим Центром сертификаты в расширение COC.

4.4.6. В случае аннулирования сертификата Пользователя Удостоверяющего Центра по истечении срока его действия временем аннулирования сертификата Пользователя Удостоверяющего Центра признается время, хранящееся в поле “Действителен по” (notAfter) поля “Срок действия сертификата” (Validity) сертификата. В данном случае информация об аннулированном сертификате Пользователя Удостоверяющего Центра в список аннулированных (отозванных) сертификатов не заносится.

4.5. **Приостановление действия сертификата открытого ключа электронной подписи**

4.5.1. Для осуществления приостановления действия сертификата открытого ключа электронной подписи пользователь подает заявление в УЦ в бумажной или электронной форме на приостановление действия сертификата.

4.5.2. Бумажная форма заявления на приостановление сертификата открытого ключа электронной подписи приведена в приложении к настоящему Регламенту.

4.5.3. Заявление на приостановление действия сертификата открытого ключа электронной подписи в электронной форме формируется и подается в УЦ с использованием программного обеспечения пользователя УЦ. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи пользователя.

4.5.4. Действие сертификата приостанавливается на исчисляемый в календарных днях срок.

4.5.5. Минимальный срок приостановления действия сертификата составляет 10 дней.

4.5.6. Подача заявления на приостановление действия сертификата, оформленного в бумажном виде, в УЦ и его рассмотрение осуществляется в течение рабочего дня.

4.5.7. Обработка заявления на приостановление действия сертификата и оповещение пользователя о приостановлении действия сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в УЦ.

4.5.8. Временем приостановления действия сертификата открытого ключа электронной подписи признается время официального уведомления пользователя о приостановлении действия данного сертификата.

4.5.9. Временем подписания электронного документа, на основании которого было проведено приостановление действия сертификата открытого ключа электронной подписи пользователя, считается время внесения документа в реестр УЦ.

4.5.10. В случае если в течение срока приостановления действия сертификата открытого ключа электронной подписи пользователя в УЦ не поступает заявление от пользователя УЦ о возобновлении действия сертификата, сертификат аннулируется (отзывается) УЦ.

4.6. **Возобновление действия сертификата открытого ключа электронной подписи**

4.6.1. Для осуществления возобновления действия сертификата открытого ключа электронной подписи пользователь подает заявление в УЦ в бумажной или электронной форме на возобновление действия сертификата.

4.6.2. Бумажная форма заявления на возобновление сертификата открытого ключа электронной подписи приведена в Приложении к настоящему Регламенту.

4.6.3. Заявление на возобновление действия сертификата открытого ключа электронной подписи в электронной форме формируется и подается в УЦ с использованием программного обеспечения пользователя УЦ. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись осуществляется на действующем ключе электронной подписи пользователя.

4.6.4. Подача заявления на возобновление действия сертификата в УЦ и его рассмотрение осуществляется только в течение рабочего дня.

4.6.5. Обработка заявления на возобновление действия сертификата и оповещение пользователя о возобновлении действия сертификата должны быть осуществлены не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в УЦ.

4.6.6. Временем возобновления действия сертификата открытого ключа электронной подписи признается время официального уведомления пользователя о возобновлении действия данного сертификата.

4.6.7. Временем подписания электронного документа, на основании которого было проведено возобновление действия сертификата открытого ключа проверки электронной подписи пользователя, считается время внесения документа в реестр УЦ.

4.6.8. Возобновление действия сертификата открытого ключа электронной подписи возможно только в течение срока, на который было приостановлено действие сертификата.

4.7. **Оплата**

4.7.1. УЦ осуществляет свою деятельность на платной основе.

4.7.2. Расчет между Пользователем УЦ и УЦ производится по тарифам, указанным на официальном сайте УЦ на день выставления счета. Оплата осуществляется в безналичном порядке с использованием платежных поручений или иным способом, предусмотренным законодательством ПМР, в рублях ПМР или в иностранной валюте в соответствии с тарифами, указанными на официальном сайте УЦ на день выставления счета.

4.7.3. Стоимость, сроки и порядок расчетов за оказанные услуги УЦ могут регулироваться отдельным соглашением между УЦ и непосредственно Пользователем УЦ.

4.7.4. В случае выполнения внеплановой смены ключей Уполномоченного лица УЦ (согласно процедуре, определенной Регламентом) УЦ выполняет изготовление сертификатов открытых ключей электронной подписи Пользователей УЦ безвозмездно.

4.7.5. Предоставление участникам информационных систем копий сертификатов открытых ключей электронной подписи Пользователей УЦ, находящихся в реестре изготовленных сертификатов, а также информации об их действии в виде Списков отозванных сертификатов в форме электронных документов осуществляется безвозмездно.

4.8. **Токены**

4.8.1. Для создания, открытого и закрытого ключей, создания ЭП, а также совершения иных действий в рамках возможностей Токена Пользователь УЦ использует Токен.

4.8.2. Удостоверяющий центр выдает Токен Пользователю УЦ по его запросу. В работе с Токеном Пользователь УЦ обязуется руководствоваться Инструкцией по работе с Токенами, опубликованной на сайте УЦ, по адресу http://ca.idc.md/documents.

4.8.3. УЦ передает Токен Пользователю УЦ по акту приема-передачи. При приеме Токена Пользователь обязан осмотреть Токен на предмет выявления видимых признаков повреждений, и при их наличии сообщить в УЦ.

4.8.4. Пользователь обязан хранить Токен в месте, недоступном для третьих лиц, обеспечивать необходимые условия для исключения доступа к Токену третьих лиц.

4.8.5. Запрещено передавать Токен третьим лицам, а также сообщать третьим лицам ПИН-код доступа к закрытому ключу ЭП. В случае если Токен или ПИН-код станут доступны третьим лицам, Пользователь УЦ обязан обратиться в УЦ с заявлением на аннулирование сертификата открытого ключа электронной подписи в порядке, определенном в Регламенте.

УЦ обязан безвозмездно заменить поврежденный Токен на аналогичный качественный Токен, если во время подписания Акта приема-передачи будут обнаружены повреждения Токена.

4.8.6. В случае если Пользователь не осуществил все необходимые действия для получения Сертификата в течение 2 (двух) месяцев со дня подписания Акта приема-передачи Токена либо после оплаты услуг Удостоверяющего центра, УЦ не оказывает услуги по изготовлению Сертификата открытого ключа электронной подписи, сформированной с использованием такого Токена либо с использованием данных, предоставленных УЦ при регистрации Пользователя (логин и пароль) по истечении вышеуказанного срока. В таком случае денежные средства, уплаченные Пользователем, возврату не подлежат, осуществление Удостоверяющим Центром услуги по изготовлению Сертификата открытого ключа электронной подписи возможно только после повторной оплаты вознаграждения за выдачу Сертификата открытого ключа электронной подписи (при условии совершения Пользователем всех необходимых действий для получения Сертификата).

4.8.7. Изготовление Сертификата осуществляется Удостоверяющим центром после регистрации и идентификации Пользователя УЦ.

5. ПРОЧИЕ УСЛОВИЯ

5.1. **Конфиденциальность информации**

5.1.1. Типы конфиденциальной информации

5.1.1.1. Закрытый ключ электронной подписи, соответствующий сертификату открытого ключа электронной подписи Пользователя УЦ, является конфиденциальной информацией данного Пользователя УЦ. Удостоверяющий Центр не осуществляет хранение закрытых ключей электронной подписи Пользователей.

5.1.1.2. Информация о Пользователях УЦ, хранящаяся в УЦ и не подлежащая непосредственной рассылке в качестве части сертификата открытого ключа электронной подписи, считается конфиденциальной.

5.1.2. Типы информации, не являющейся конфиденциальной

5.1.2.1. Информация, не являющаяся конфиденциальной информацией, считается открытой информацией.

5.1.2.2. Открытая информация может публиковаться по решению УЦ. Место, способ и время публикации открытой информации определяется УЦ.

5.1.2.3. Персональные данные, включаемые в сертификаты открытых ключей электронной подписи Пользователей УЦ и списки аннулированных сертификатов, издаваемые УЦ, относятся к общедоступным персональным данным и могут быть переданы третьим лицам в целях обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей. Обработка персональных данных УЦ осуществляется в целях выдачи сертификата открытых ключей электронной подписи, выпуска списков аннулированных сертификатов и обеспечения работоспособности и информационной целостности инфраструктуры открытых ключей.

5.1.2.4. Информация, содержащаяся в настоящем Регламенте, не считается конфиденциальной.

5.1.3. Исключительные полномочия УЦ

Удостоверяющий Центр имеет право раскрывать конфиденциальную информацию третьим лицам только в случаях, установленных законодательством ПМР.

5.2. **Плановая смена ключей уполномоченного лица Удостоверяющего Центра**

Плановая смена ключей (закрытого ключа электронной подписи и соответствующего ему открытого ключа электронной подписи) Удостоверяющего Центра выполняется в период действия ключа электронной подписи Удостоверяющего центра.

Процедура плановой смены ключей Удостоверяющего Центра осуществляется в следующем порядке:

Уполномоченное лицо Удостоверяющего Центра формирует новый закрытый ключ электронной подписи и соответствующий ему открытый ключ электронной подписи;

Уполномоченное лицо Удостоверяющего Центра изготавливает сертификат нового открытого ключа электронной подписи и подписывает его электронной подписью вышестоящего по иерархии УЦ.

Старый закрытый ключ электронной подписи Удостоверяющего Центра используется в течение своего срока действия для формирования списков аннулированных сертификатов в электронной форме, изданных Удостоверяющим Центром в период действия старого закрытого ключа электронной подписи Удостоверяющего Центра.

5.3. **Компрометация закрытого ключа Удостоверяющего Центра**

В случае компрометации или угрозы компрометации закрытого ключа электронной подписи Удостоверяющего Центра выполняется внеплановая смена ключей Удостоверяющего Центра.

Процедура внеплановой смены ключей Удостоверяющего Центра выполняется в порядке, определенном процедурой плановой смены ключей Удостоверяющего Центра.

В случае компрометации ключа Удостоверяющего Центра после выполнения процедуры внеплановой смены ключей, сертификат открытого ключа электронной подписи Удостоверяющего Центра аннулируется путем занесения в реестр отозванных сертификатов лицом, выдавшим его Удостоверяющему Центру.

5.4. **Компрометация закрытого ключа Пользователя Удостоверяющего Центра**

Пользователь Удостоверяющего Центра самостоятельно принимает решение о факте или угрозе компрометации своего закрытого ключа электронной подписи.

В случае компрометации или угрозы компрометации закрытого ключа электронной подписи Пользователь подает в Удостоверяющий центр Заявление на аннулирование (отзыв) сертификата открытого ключа электронной подписи в соответствии с правилами, установленными в данном Регламенте.

5.5. **Прекращение деятельности Удостоверяющего Центра**

Прекращение деятельности Удостоверяющего Центра может быть осуществлено на основании решения Компании и в порядке, установленном внутренними документами Компании.

Все сертификаты открытого ключа электронной подписи Пользователей, выданные Удостоверяющим Центром, аннулируются.

5.6. **Опубликование и оповещение**

Удостоверяющий Центр обязан уведомить о факте аннулирования сертификата открытого ключа электронной подписи его владельца, а в случае выдачи сертификата юридическому лицу – уведомить и владельца сертификата, и юридическое лицо.

Срок уведомления – не позднее рабочего дня, следующего за рабочим днем, в течение которого было подано заявление в Удостоверяющий Центр на аннулирование сертификата.

Официальным уведомлением о факте аннулирования сертификата является опубликование списка аннулированных сертификатов, содержащего сведения об аннулированном сертификате. Временем опубликования считается время издания списка аннулированных сертификатов, указанное в поле thisUpdate изданного списка аннулированных сертификатов.

Информация о размещении списка отозванных сертификатов заносится в сертификат открытого ключа электронной подписи Пользователя Удостоверяющего Центра поле CRL Distribution Point.

5.7. **Сроки действия ключей уполномоченного лица Удостоверяющего Центра**

Срок действия ключа электронной подписи 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 Удостоверяющего Центра исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа электронной подписи.

Срок действия сертификата открытого ключа электронной подписи, соответствующего закрытому ключу электронной подписи Удостоверяющего Центра, составляет 10 лет.

5.8. **Сроки действия ключей Пользователей**

Установленные сроки действия ключей электронной подписи и сертификатов открытого ключа электронной подписи приведены в приложении к данному Регламенту.

Начало периода действия ключа электронной подписи Пользователя исчисляется с даты и времени начала действия соответствующего сертификата открытого ключа электронной подписи.

5.9. **Хранение сертификатов открытого ключа электронной подписи в Удостоверяющем Центре**

Срок хранения сертификата открытого ключа электронной подписи в Удостоверяющем Центре осуществляется в течение всего периода его действия и 5 лет после его аннулирования (отзыва).

По истечении указанного срока хранения сертификаты открытого ключа электронной подписи переводятся в режим архивного хранения.

5.10. **Структура сертификата открытого ключа электронной подписи и списков отозванных сертификатов**

Удостоверяющий Центр издает сертификаты открытых ключей электронной подписи Пользователей в электронной форме формата X.509 версии 3 и список отозванных сертификатов (COC) в электронной форме формата X.509 версии 2.

5.10.1. Структура сертификата открытого ключа электронной подписи УЦ

Название	Описание	Содержание
Базовые поля сертификата		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номера сертификата
Signature Algorithm	Алгоритм подписи	Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer	Издатель сертификата	CN = IDC Root CA OU = IT Department O = Interdnestrcom JSC L = Tiraspol S = PMR C = MD
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = IDC Issuer CA OU = IT Department O = Interdnestrcom JSC L = Tiraspol S = PMR C = MD
Public Key	Открытый ключ электронной подписи	Открытый ключ сертификата
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	Алгоритм подписи Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer Sign	ЭП издателя сертификата	Подпись издателя в соответствии с sha256 RSA
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 ключа электронной подписи Удостоверяющего Центра, соответствующего данному сертификату
Certificate Policies	Политики сертификата 2.5.29.32	[1] Политика сертификата Идентификатор политики=1.3.6.1.4.1.58637.1.1 Interdnestrcom CPS

		[2] Размещение CPS: https://ca.idc.md/pki/polices.html
BasicConstraints	Основные ограничения	SybjectType (Тип владельца сертификата) = CA Path Length Constraint (Ограничение на длину пути – ограничивает количество уровней иерархии при создании подчиненных Удостоверяющих Центров) = 0
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата	Версия сертификата Уполномоченного лица Удостоверяющего Центра
Thumbprint Algorithm	Алгоритм хэш-функции сертификата	sha1
Thumbprint	Значение хэш-функции сертификата	Значение хэш-функции сертификата в соответствии с алгоритмом sha1

5.10.2. Структура списка аннулированных сертификатов Удостоверяющего Центра

Название	Описание	Содержание
Базовые поля списка аннулированных сертификатов		
Version	Версия	V2
Issuer	Издатель CAC	CN = IDC Issuer CA OU = IT Department O = Interdnestrcom JSC L = Tiraspol S = PMR C = MD
thisUpdate	Время издания CAC	дд.мм.гггг чч:мм:сс GMT
nextUpdate	Время, по которое действителен CAC	дд.мм.гггг чч:мм:сс GMT
revokedCertificates	Список отозванных сертификатов	Последовательность элементов следующего вида: Серийный номер сертификата (CertificateSerialNumber) Время обработки заявления на аннулирование (отзыв) и приостановление действия сертификата (Time)
signatureAlgorithm	Алгоритм подписи	Алгоритм подписи уполномоченного лица Удостоверяющего Центра, соответствующий требованиям Регламента
Issuer Sign	Подпись издателя CAC	Подпись издателя в соответствии с sha256
Расширения списка аннулированных сертификатов		
Reason Code	Код причины аннулирования сертификата	"0" – Не указана "1" – Компрометация ключа "2" – Компрометация ключа электронной подписи уполномоченного лица Удостоверяющего Центра "3" – Изменение принадлежности "4" – Сертификат заменен "5" – Прекращение работы
Authority Key Identifier	Идентификатор ключа издателя	Идентификатор ключа электронной подписи уполномоченного лица Удостоверяющего Центра, на котором подписан COC
SzOID_CertSrv_CA_Version	Объектный идентификатор сертификата издателя	Версия сертификата Уполномоченного лица Удостоверяющего Центра

6. РАЗРЕШЕНИЕ СПОРОВ

При возникновении споров, стороны предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящего Регламента, путем переговоров.

7. РИСКИ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННОЙ ПОДПИСИ

При использовании ЭП Пользователь должен учитывать, возникновение следующих явных рисков:

7.1. Риски, связанные с несоответствием условий использования электронной подписи установленному порядку.

В случае использования электронной подписи в порядке, не соответствующем требованиям законодательства ПМР или соглашений между участниками электронного взаимодействия, юридическая сила подписанных в данном случае документов может быть поставлена под сомнение.

7.2. Риски, связанные с компрометацией закрытого ключа ЭП или несанкционированным доступом к средствам ЭП.

В данном случае может быть получен документ, порождающий юридически значимые последствия и исходящий от имени Пользователя, закрытый ключ которого был скомпрометирован.

8. ОТВЕТСТВЕННОСТЬ СТОРОН

8.1. **Ответственность за неисполнение**

УЦ не несет ответственность за неисполнение либо ненадлежащее исполнение своих обязанностей по настоящему Регламенту, а также возникшие в связи с этим убытки в случаях:

− подделки, подлога либо иного искажения присоединившейся Стороной, Владельцем Сертификата либо третьими лицами информации, содержащейся в заявлениях либо иных документах, представленных в УЦ;

− если Пользователь не исполняет или ненадлежащим образом исполняет свои обязанности, что делает невозможным исполнение УЦ своих обязанностей;

− если Пользователь своевременно не осуществил процедуру по аннулированию Сертификата при компрометации закрытого ключа электронной подписи.

8.2. **Ответственность за убытки**

УЦ несет ответственность за убытки, возникшие вследствие компрометации закрытого ключа электронной подписи уполномоченного лица УЦ, либо вследствие несоответствия сведений в Сертификате сведениям, указанным в заявлении на выдачу Сертификата.

8.3. Ответственность Удостоверяющего Центра регулируется законодательством ПМР.

9. СОГЛАСИЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ ПО КАНАЛАМ СВЯЗИ И ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Присоединяясь к Регламенту УЦ, Пользователь УЦ выражает свое согласие на получение от Удостоверяющего центра информационных и рекламных рассылок, путем осуществления прямых контактов с использованием всех средств связи, включая, но не ограничиваясь: почтовая рассылка, СМС-рассылка, голосовая рассылка, рассылка электронных писем.

9.2. Присоединяясь к Регламенту, Пользователь УЦ, в соответствии с Законом ПМР «О персональных данных», в целях регистрации и обслуживания в УЦ (формирования общедоступных справочников сертификатов открытых ключей электронной подписи) выражает согласие УЦ на обработку им (сбор, систематизация, накопление, хранение, изменение, использование, обезличивание, блокирование, уничтожение) своих персональных данных с использованием или без использования средств автоматизации, а именно: фамилия, имя, отчество, дата рождения, место жительство, реквизиты паспорта (серия, номер, орган его выдавший, дата выдачи), номер телефона.

10. РЕКВИЗИТЫ УЦ

СЗАО «Интерднестрком», именуемое в дальнейшем «Удостоверяющий Центр», зарегистрировано на территории ПМР.

Свидетельство о регистрации серии АА №0010133 выдано 08.10.1998 (регистрационный номер №01-022-1759).

Удостоверяющий Центр в качестве участника рынка услуг по изготовлению и выдаче сертификатов ключей электронной подписи осуществляет свою деятельность на территории ПМР на основании Приказа Министерства цифрового развития, связи и коммуникаций ПМР от 18.07.2023 года №224 (номер и дата аккредитации Удостоверяющего центра №3 от 18.07.2023г.).

Юридический адрес: 3300, г. Тирасполь, ул. Восстания, 41, ПМР.

ПРИЛОЖЕНИЕ №1
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

ПОРЯДОК РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА, СОЗДАНИЯ КЛЮЧЕВЫХ ДАННЫХ И ВЫДАЧИ, АННУЛИРОВАНИЯ, ПРИОСТАНОВЛЕНИЯ ДЕЙСТВИЯ И ВОЗОБНОВЛЕНИЯ ДЕЙСТВИЯ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА ЭЛЕКТРОННОЙ ПОДПИСИ

1. Регистрация заявителей, генерация ключевой информации, изготовление и получение первого сертификата открытого ключа электронной подписи заявителя.

1.1. Заявитель, желающий пройти процедуру регистрации в УЦ, должен явиться лично в Удостоверяющий центр, представить перечень документов, определенных в настоящем Регламенте, и подписать заявление по форме, установленной настоящим Регламентом, собственноручной подписью и печатью (для юридических лиц (для органов государственной власти допускается изготовление заявления без проставления оттиска печати, в случае использования фирменного (нумерованного бланка).

1.2. **Перечень документов для регистрации и идентификации Пользователя:**

1.2.1. Перечень документов, необходимых для юридического лица (за исключением органов государственной власти и управления):

- выписка из ГРЮЛ, выданная не позднее, чем за 10 календарных дней до даты обращения в УЦ;
- паспорт лица (удостоверение личности), обладающего правом на представление интересов юридического лица без доверенности;
- справка из обслуживающего банка об открытии счетов.

В случае обращения за регистрацией иного лица, не указанного в выписке из ГРЮЛ, дополнительно предоставляется:

- паспорт (удостоверение личности) представителя заявителя.
- доверенность представителя.

1.2.2. Перечень документов, необходимых для органов государственной власти и управления:

- паспорт лица (удостоверение личности), обладающего правом на представление интересов органов государственной власти и управления без доверенности;
- заверенная копия документа о назначении на должность руководителя органа государственной власти и управления;
- заверенная копия сертификата о присвоении фискального кода (иной документ, свидетельствующий о присвоении фискального кода).
- справка из обслуживающего банка об открытии счетов.

В случае обращения за регистрацией иного лица, не являющегося руководителем органа государственной власти и управления, дополнительно предоставляются:

- паспорт (удостоверение личности) представителя заявителя;
- доверенность представителя.

При обращении представителя организации паспорт руководителя юридического лица, органа государственной власти и управления не предоставляется.

1.2.3. Перечень документов, необходимых для физических лиц:

- паспорт (удостоверение личности);
- свидетельство о регистрации по месту жительства (при отсутствии штампа в паспорте).

1.2.4. Перечень документов, необходимых для специального субъекта:

- паспорт (удостоверение личности);
- свидетельство о регистрации по месту жительства (при отсутствии штампа в паспорте);
- удостоверение (иной документ, свидетельствующий о специальном статусе).

1.3. **Оператор Удостоверяющего центра:**

1.3.1. осуществляет идентификацию Пользователя путем установления личности (по документу, удостоверяющему личность);

1.3.2. В случае положительной идентификации лица, проходящего процедуру регистрации, проверяет состав, полноту и корректность предоставленных документов;

1.3.3. В случае отсутствия ошибок, оператор УЦ формирует и отправляет запрос в систему МВД для получения идентификационного номера физического лица;

1.3.4. При получении идентификационного номера физического лица:

1.3.4.1. Вносит в систему УЦ данные заявителя;

1.3.4.2. Формирует заявление на регистрацию и присоединение к Регламенту и изготовление сертификата открытого ключа электронной подписи в УЦ, распечатывает его и передает Заявителю для проверки и подписания;

1.3.5. Принимает подписанное заявление;

1.3.6. Фотографирует заявителя с заявлением на регистрацию и присоединение к Регламенту;

1.3.7. При запросе Заявителя на выдачу токена – осуществляет мероприятия по выдаче токена;

1.3.8. Предоставляет счет на оплату услуг Удостоверяющего центра;

1.3.9. После оплаты услуг Удостоверяющего центра предоставляет Заявителю данные для входа в личный кабинет Пользователя и формирования запроса на изготовление сертификата открытого ключа электронной подписи;

1.3.10. Разъясняет порядок осуществления мероприятий по формированию электронного запроса на изготовление сертификата открытого ключа электронной подписи;

1.3.11. При поступлении электронного запроса от Пользователя, идентификации системой Пользователя - одобряет электронный запрос заявителя на изготовление сертификата открытого ключа электронной подписи в УЦ.

В случае нахождения недостоверных или ошибочных сведений, отказа в предоставлении идентификационного номера физического лица, недостаточности документов, заявление на регистрацию, присоединение к Регламенту и создание и выдачу сертификата открытого ключа электронной подписи не формируется с указанием оператором УЦ причины отказа в оказании услуги.

1.4. **Порядок изготовления открытого ключа электронной подписи**

1.4.1. Пользователь УЦ на своем рабочем месте с помощью программного обеспечения УЦ - “IDC: Управления ключами” инициирует запрос на изготовление сертификата открытого ключа электронной подписи в формате PKCS#10. В процессе формирования запроса программное обеспечение УЦ с помощью средств электронной подписи генерирует ключевую информацию и формирует на токене контейнер закрытого ключа электронной подписи.

1.4.2. Сформированный запрос на изготовление сертификата открытого ключа электронной подписи регистрируется в системе УЦ.

1.4.3. Пользователь УЦ на своем рабочем месте с помощью программного обеспечения УЦ - “IDC: Управления ключами” импортирует полученный сертификат открытого ключа электронной подписи на токен.

2. Генерация ключей электронной подписи пользователей УЦ

Генерация ключа электронной подписи пользователя УЦ осуществляется в следующих случаях:

- при формировании первого ключа электронной подписи заявителя;
- при плановой смене ключа электронной подписи пользователя УЦ.

В указанных случаях программное обеспечение УЦ с помощью средств электронной подписи по запросу пользователя УЦ генерирует ключевую информацию и формирует на токене контейнер закрытого ключа электронной подписи.

3. Изготовление и получение последующих сертификатов открытого ключа электронной подписи пользователя УЦ

Формирование сертификата открытого ключа электронной подписи Пользователя УЦ осуществляется УЦ на основании электронного запроса в формате PKCS#10 на создание и выдачу сертификата открытого ключа электронной подписи, который направляется с использованием программного обеспечения УЦ - “IDC: Управления ключами”.

Запрос на создание сертификата открытого ключа электронной подписи Пользователя УЦ при плановой смене сертификата ключа электронной подписи представляет собой запрос в электронной форме в формате PKCS#10, который направляется с использованием программного обеспечения УЦ.

УЦ осуществляет создание сертификата открытого ключа электронной подписи в виде электронного документа в соответствии с поступившим запросом.

При плановой смене сертификата ключа электронной подписи значения полей Subject, Key Usage, Extended Key Usage изготовленного сертификата идентичны значениям этих полей в сертификате, который подвергся смене.

Срок создания сертификата открытого ключа электронной подписи не может превышать 3 рабочих дней с момента поступления электронного запроса на создание сертификата в УЦ.

Сертификат открытого ключа электронной подписи направляется его владельцу с использованием программного обеспечения УЦ - “IDC: Управления ключами”.

4. Формирование и передача заявления на аннулирование сертификата открытого ключа электронной подписи в электронной форме

Заявление на аннулирование сертификата открытого ключа электронной подписи формируется Пользователем УЦ и направляется в электронном виде в УЦ с использованием программного обеспечения УЦ - “IDC: Управление ключами”.

Заявление на аннулирование сертификата открытого ключа электронной подписи представляет собой электронный документ формата XAdES. В качестве подписываемых данных используется запрос на аннулирование сертификата, а электронная подпись осуществляется в соответствии с установленным порядком на действующем ключе электронной подписи Пользователя УЦ, либо на ключе электронной подписи уполномоченного лица Компании.

Запрос на аннулирование сертификата открытого ключа электронной подписи представляет собой строку формата XML со следующими атрибутами: CertificateSerialNumber, ReasonCode, SomeComment, SecretPhrase, где:

CertificateSerialNumber - серийный номер аннулируемого сертификата открытого ключа электронной подписи;

ReasonCode − код причины аннулирования из следующего перечня допустимых значений:

"0" − Не указана

"1" − Компрометация ключа

"2" − Компрометация ключа электронной подписи Удостоверяющего Центра.

"3" − Изменение принадлежности

"4" − Сертификат заменен

"5" − Прекращение работы

SomeComment − текстовое значение комментария владельца сертификата открытого ключа электронной подписи;

SecretPhrase – секретное слово владельца сертификата открытого ключа электронной подписи переданного в запросе на создание сертификата открытого ключа, действие которого необходимо аннулировать.

5. Формирование и передача заявления на приостановление действия сертификата открытого ключа электронной подписи

Заявление на приостановление действия сертификата открытого ключа электронной подписи формируется и направляется в электронном виде в УЦ с использованием программного обеспечения УЦ - “IDC: Управления ключами”.

Заявление на приостановление действия сертификата открытого ключа электронной подписи представляет собой электронный документ формата XAdES. В качестве подписываемых данных используется запрос на приостановление действия сертификата, а электронная подпись осуществляется в соответствии с установленным порядком на действующем ключе электронной подписи Пользователя, либо на ключе электронной подписи уполномоченного лица Компании.

Запрос на приостановление действия сертификата открытого ключа электронной подписи представляет собой строку формата XML со следующими атрибутами: CertificateSerialNumber, ReasonCode, SomeComment, SecretPhrase, где:

CertificateSerialNumber - серийный номер сертификата открытого ключа электронной подписи, действие которого необходимо приостановить;

ReasonCode − код причины: "6" (приостановление действия сертификата);

SomeComment − текстовое значение комментария владельца сертификата открытого ключа электронной подписи;

SecretPhrase – секретное слово владельца сертификата открытого ключа электронной подписи переданного в запросе на создание сертификата открытого ключа, действие которого необходимо приостановить.

6. Формирование и передача заявления на возобновление действия сертификата открытого ключа электронной подписи в электронной форме

Заявление на возобновление действия сертификата открытого ключа электронной подписи формируется и направляется в электронном виде в УЦ с использованием программного обеспечения УЦ - “IDC: Управления ключами”.

Заявление на возобновление действия сертификата открытого ключа электронной подписи в электронной форме представляет собой электронный документ формата XAdES. В качестве подписываемых данных используется запрос на возобновление действия сертификата, а электронная подпись осуществляется в соответствии с установленным порядком на действующем ключе электронной подписи Пользователя, либо на ключе электронной подписи уполномоченного лица Компании.

Запрос на возобновление действия сертификата открытого ключа электронной подписи представляет собой строку формата XML с атрибутом CertificateSerialNumber, где:

CertificateSerialNumber - серийный номер сертификата открытого ключа электронной подписи, действие которого необходимо возобновить.

7. Сроки действия ключей электронной подписи и сертификата открытого ключа электронной подписи Пользователей

Срок действия ключа электронной подписи и сертификата открытого ключа электронной подписи Пользователя Удостоверяющего Центра – 1 год.

Название	Описание	Содержание
Базовые поля сертификата открытого ключа электронной подписи		
Version	Версия	V3
Serial Number	Серийный номер	Уникальный серийный номер сертификата
Signature Algorithm	Алгоритм подписи	Алгоритм подписи уполномоченного лица УЦ, соответствующий требованиям Регламента
Issuer	Издатель сертификата	CN = IDC Issuer CA OU = IT Department O = Interdnestrcom JSC L = Tiraspol S = PMR C = MD
Validity Period	Срок действия сертификата	Действителен с: дд.мм.гггг чч:мм:сс GMT Действителен по: дд.мм.гггг чч:мм:сс GMT
Subject	Владелец сертификата	CN = Общее имя = Фамилия, Имя, Отчество O = Организация владельца сертификата L = Город владельца сертификата C = Страна владельца сертификата E = Электронная почта владельца сертификата
Public Key	Открытый ключ электронной подписи	Открытый ключ электронной подписи (Алгоритм подписи УЦ, соответствующий требованиям Регламента)
Issuer Signature Algorithm	Алгоритм подписи издателя сертификата	Алгоритм подписи УЦ, соответствующий требованиям Регламента
Issuer Sign	ЭП издателя сертификата	Sha256 RSA

Дополнения сертификата открытого ключа электронной подписи		
Certificate Policies	Политика сертификата 2.5.29.32	[1] Политика сертификата: Идентификатор политики=1.3.6.1.4.1.58637.1.1 Interdnestrcom CPS, Класс средства УЦ КС2 [2] Размещение CPS: https://ca.idc.md/pki/polices.html
Key Usage (critical)	Использование ключа 2.5.29.15	Неотрекаемость – невозможность осуществления отказа от совершенных действий; Подпись, Шифрование ключей, Шифрование данных
Extended Key Usage	Улучшенный ключ 2.5.29.37	Набор идентификаторов (OID), определяющий отношения, при осуществлении которых электронный документ с электронной подписью будет иметь юридическое значение
Subject Key Identifier	Идентификатор ключа владельца сертификата 2.5.29.14	Идентификатор ключа электронной подписи владельца сертификата
Authority Key Identifier	Идентификатор ключа издателя сертификата 2.5.29.35	Идентификатор ключа электронной подписи УЦ
CRL Distribution Point	Точка распределения списка отозванных сертификатов (CRL) 2.5.29.31	http://ca.idc.md/ext/IDC_Issuer_CA.crl
Thumbprint Algorithm	Алгоритм хэш-функции сертификата	Sha1
Thumbprint	Значение хэш-функции сертификата	Значение хэш-функции сертификата открытого ключа электронной подписи в соответствии с алгоритмом Sha1
1.3.6.1.4.1.58637.2.1.1	Идентификатор клиента в системе УЦ	UTF8String: ClientId=<Идентификатор клиента>
1.3.6.1.4.1.52072.1.1	Единый регистрационный номер физического лица	IA5String
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица, только для юридических лиц	IA5String
1.3.6.1.4.1.52072.1.3	Фискальный код государственного учреждения	IA5String

ПРИЛОЖЕНИЕ №2
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Области действия сертификатов открытых ключей электронной подписи

1. Принципы построения объектных идентификаторов областей применения сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра Компании (OID).

Международной ассоциацией IANA за Компанией зарегистрировано значение 1.3.6.1.4.1. 58637.

В качестве корневого объектного идентификатора для построения структуры идентификаторов областей применения сертификатов открытых ключей электронной подписи Удостоверяющим Центром используется значение, зарегистрированное в международной ассоциации IANA.

Структура объектных идентификаторов областей применения сертификатов открытых ключей электронной подписи Пользователей Удостоверяющего Центра имеет вид:

1.3.6.1.4.1. 58637.X.YY, где:

- **X** – Бизнес-система, обозначаемая одним из следующих числовых значений:

1 – Системный раздел

2 – Сертификаты открытого ключа ЭП физических и юридических лиц

- **YY** – Области применения сертификатов, относящиеся к Компании:

Области применения сертификатов, принадлежащих Удостоверяющему центру:

OID	Название	Область действия
1.3.6.1.4.1.58637.1	**Системный раздел**	
1.3.6.1.4.1.58637.1.1	Политики сертификатов в CPS	Ссылка на опубликованные политики выдачи сертификатов центром сертификации Компании
1.3.6.1.4.1.58637.1.2	Политики сервера штампов времени	
1.3.6.1.4.1.58637.1.2.1	RSA 2048	Алгоритм подписи штампа времени
1.3.6.1.4.1.58637.2	**Сертификаты Пользователей**	
1.3.6.1.4.1.58637.2.1	Сертификат пользователя УЦ	
1.3.6.1.4.1.58637.2.1.1	Сертификат Пользователя	Расширение сертификата для идентификации клиента либо подписи электронных документов. Область действия Сертификата устанавливается на основании заявлений Пользователей

Технологические объекты сертификатов открытых ключей электронной подписи (принадлежат Министерству цифрового развития, связи и массовых коммуникаций ПМР):

Объектный идентификатор (OID)	**Название**
1.3.6.1.4.1.52072.1.1	Идентификатор физического лица
1.3.6.1.4.1.52072.1.2	Регистрационный номер юридического лица
1.3.6.1.4.1.52072.1.3	Сертификат органа государственной, исполнительной власти или органа местного самоуправления
1.3.6.1.4.1.52072.1.4	Специальный Сертификат
1.3.6.1.4.1.52072.2.1	Сертификат оператора фискальных данных
1.3.6.1.4.1.52072.2.2	Сертификат кассы ОФД

ПРИЛОЖЕНИЕ №3а
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для юридических лиц

Заявление
о регистрации, присоединении
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»
и создание и выдачу сертификата открытого ключа электронной подписи

_____,
(полное наименование юридического лица)

в лице _____
(должность, Ф.И.О. уполномоченного лица)

действующего на основании _____
(наименование и дата документа)

1) просит произвести регистрацию в Удостоверяющем центре в соответствии с указанными в настоящем заявлении данными:

сведения о юридическом лице	
Полное наименование юридического лица	
Сокращенное наименование юридического лица	
Юридический адрес юридического лица	
Почтовый адрес юридического лица	
Регистрационный номер	
Банковские реквизиты:	
наименование Банка	
номер счета	
Фискальный код (для органов государственной власти и управления)	
сведения об уполномоченном представителе / руководителе юридического лица	
ФИО (полностью)	
дата рождения	
данные паспорта (удостоверения личности) (номер, серия, дата выдачи)	
должность	
доверенность (номер, дата (при наличии доверенности, срок действия)	
контактные данные	
ФИО (полностью)	
номер телефона (с кодом города)	
e-mail	

2) полностью и безусловно присоединяется к Регламенту Удостоверяющего центра СЗАО «Интерднестрком», условия которого определены СЗАО «Интерднестрком» и опубликованы на сайте Удостоверяющего центра СЗАО «Интерднестрком» по адресу http://ca.idc.md;

3) свидетельствует о том, что с Регламентом Удостоверяющего центра СЗАО «Интерднестрком» и приложениями к нему ознакомлен, согласен и обязуется соблюдать все положения указанного документа;

4) просит создать и выдать сертификат открытого ключа электронной подписи (далее – «Сертификат»).

Я заявляю, что любые действия, которые будут мной совершены на основании этого Сертификата, являются действиями, совершаемыми от моего имени.

Настоящим принимаю и соглашаюсь с тем, что в случаях обнаружения недостоверности сведений, указанных в настоящем Заявлении, а также в иных случаях, установленных действующим

законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра СЗАО «Интерднестрком», выданный Сертификат может быть аннулирован Удостоверяющим центром СЗАО «Интерднестрком».

Заявитель:

_____

(наименование юридического лица)

_____

(должность, ФИО уполномоченного лица)

_____

(подпись) (фамилия)

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /

(подпись) *(фамилия, имя, отчество)*

М.П.

ПРИЛОЖЕНИЕ №3б
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для физических лиц

Заявление
о регистрации, присоединении
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»
и создание и выдачу сертификата открытого ключа электронной подписи

Я, _____
ФИО

1) прошу произвести регистрацию в Удостоверяющем центре в соответствии с указанными в настоящем заявлении данными:

ФИО (полностью)	
дата рождения	
данные паспорта (удостоверения личности) (номер, серия, дата выдачи)	
место жительства (регистрации)	
Банковские реквизиты:	
наименование Банка	
номер счета	
место работы *(по желанию)*	
контактные данные	
номер телефона (с кодом города)	
e-mail	

2) полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра СЗАО «Интерднестрком», условия которого определены СЗАО «Интерднестрком» и опубликованы на сайте Удостоверяющего центра СЗАО «Интерднестрком» по адресу http://ca.idc.md;

3) свидетельствую о том, что с Регламентом Удостоверяющего центра СЗАО «Интерднестрком» и приложениями к нему ознакомлен, согласен и обязуюсь соблюдать все положения указанного документа;

4) прошу создать и выдать сертификат открытого ключа электронной подписи (далее – «Сертификат»).

Я заявляю, что любые действия, которые будут мной совершены на основании этого Сертификата, являются действиями, совершаемыми от моего имени.

Настоящим принимаю и соглашаюсь с тем, что в случаях обнаружения недостоверности сведений, указанных в настоящем Заявлении, а также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра СЗАО «Интерднестрком», выданный Сертификат может быть аннулирован Удостоверяющим центром СЗАО «Интерднестрком».

Заявитель:

_____

(подпись) (фамилия)

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____

(подпись) (ФИО) М.П.

ПРИЛОЖЕНИЕ №3в
к Регламенту Удостоверяющего центра СЗАО «Интерднестркom»

Для физических лиц: нотариус, частный нотариус, судебный исполнитель, следователь, дознаватель, налоговый инспектор

Заявление
о регистрации, присоединении
к Регламенту Удостоверяющего центра СЗАО «Интерднестркom»
и создание и выдачу сертификата открытого ключа электронной подписи

Я, _____
ФИО

1) прошу произвести регистрацию в Удостоверяющем центре в соответствии с указанными в настоящем заявлении данными:

ФИО (полностью)	
дата рождения	
данные паспорта (удостоверения личности) (номер, серия, дата выдачи)	
место жительства (регистрации)	
Банковские реквизиты:	
наименование Банка	
номер счета	
правовой статус (с указанием номера удостоверения, иного документа, даты выдачи, срока действия (при наличии)	
контактные данные	
номер телефона (с кодом города)	
e-mail	

2) полностью и безусловно присоединяюсь к Регламенту Удостоверяющего центра СЗАО «Интерднестркom», условия которого определены СЗАО «Интерднестркom» и опубликованы на сайте Удостоверяющего центра СЗАО «Интерднестркom» по адресу http://ca.idc.md;

3) свидетельствую о том, что с Регламентом Удостоверяющего центра СЗАО «Интерднестркom» и приложениями к нему ознакомлен, согласен и обязуюсь соблюдать все положения указанного документа;

4) прошу создать и выдать сертификат открытого ключа электронной подписи (далее – «Сертификат»).

Я заявляю, что любые действия, которые будут мной совершены на основании этого Сертификата, являются действиями, совершаемыми от моего имени.

Настоящим принимаю и соглашаюсь с тем, что в случаях обнаружения недостоверности сведений, указанных в настоящем Заявлении, а также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра СЗАО «Интерднестркom», выданный Сертификат может быть аннулирован Удостоверяющим центром СЗАО «Интерднестркom».

Заявитель:

_____
(подпись) (ФИО)

Принято:
Удостоверяющий центр СЗАО «Интерднестркom»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____
(подпись) (ФИО) М.П.

ПРИЛОЖЕНИЕ №3г
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для юридических лиц

Заявление
на аннулирование сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____20__ г.

_____
(наименование юридического лица),

в лице _____
(должность, Ф.И.О. уполномоченного лица)

действующего на основании _____
(наименование документа и дата совершения (в отношении доверенности)

просит аннулировать Сертификат открытого ключа электронной подписи (далее – «Сертификат»), выданный _____
(наименование юридического лица)

в Удостоверяющем центре СЗАО «Интерднестрком», владельцем которого является

_____
(Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда выдан)

Данные Сертификата:

Идентификатор открытого ключа:

_____

в связи с _____
(причина аннулирования Сертификата)

Заявитель (владелец сертификата):

_____
(наименование юридического лица)

_____
(должность)

_____ /_____
(подпись) (фамилия, имя, отчество)

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____
(подпись) (фамилия, имя, отчество)

М.П.

ПРИЛОЖЕНИЕ №3д
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для физических лиц и лиц, которым выдан специальный сертификат

Заявление
на аннулирование сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____202_ г.

Я, _____
(ФИО)

_____
(наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан)

являющийся владельцем Сертификата открытого ключа электронной подписи (далее – «Сертификат»), выданным Удостоверяющим центром СЗАО «Интерднестрком», прошу аннулировать Сертификат.

Данные Сертификата:

Идентификатор открытого ключа

_____

в связи с _____
(причина аннулирования Сертификата)

Владелец Сертификата:

_____
_____ /
(подпись) *(фамилия, имя, отчество)*

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /
(подпись) *(фамилия, имя, отчество)*

М.П.

ПРИЛОЖЕНИЕ №3е
к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для юридических лиц

Заявление
на приостановление действия сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____202_ г.

_____
(наименование юридического лица),

в лице _____
(должность, Ф.И.О. уполномоченного лица)

действующего на основании _____
(наименование документа и дата совершения (в отношении доверенности)

просит приостановить действие Сертификата открытого ключа электронной подписи (далее – «Сертификат»),
выданный _____
(наименование юридического лица)

в Удостоверяющем центре СЗАО «Интерднестрком», владельцем которого является

_____
(Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда выдан)

Данные Сертификата:

Идентификатор открытого ключа _____

_____

в связи с _____

Срок приостановления действия сертификата _____ календарных дней.
(количество дней прописью)

Владелец сертификата:

_____
(наименование юридического лица)

_____
(должность)

_____ /
(подпись) (фамилия, имя, отчество)

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____
(подпись) (фамилия, имя, отчество)

М.П.

ПРИЛОЖЕНИЕ №3ж

к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»
Для физических лиц и лиц, которым выдан специальный сертификат

Заявление
на приостановление сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____202_ г.

Я, _____
(ФИО)

_____
(наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан)

прошу приостановить действие Сертификата открытого ключа электронной подписи (далее – «Сертификат»),

Данные Сертификата:

Идентификатор открытого ключа

_____

в связи с _____

Срок приостановления действия сертификата _____ календарных дней.
(количество дней прописью)

Владелец сертификата:

_____
_____
_____
_____ /
(подпись) *(фамилия, имя, отчество)*

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____
(подпись) *(фамилия, имя, отчество)*

М.П.

ПРИЛОЖЕНИЕ №3з

к Регламенту Удостоверяющего центра СЗАО «Интерднестрком»

Для юридических лиц

Заявление
на возобновление действия сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____202_ г.

_____
(наименование юридического лица),

в лице _____
(должность, Ф.И.О. уполномоченного лица)

действующего на основании _____
(наименование документа и дата совершения (в отношении доверенности)

просит возобновить действие Сертификата открытого ключа электронной подписи (далее – «Сертификат»), выданный _____ (наименование юридического лица) в Удостоверяющем центре СЗАО «Интерднестрком», владельцем которого является

_____
(Ф.И.О., документ удостоверяющий личность, его серия и номер, кем и когда выдан)

Данные Сертификата:

Идентификатор открытого ключа

_____

Владелец сертификата:

_____
_____
(наименование юридического лица)
_____
(должность)
_____
(подпись) (фамилия, имя, отчество)

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /_____
(подпись) (фамилия, имя, отчество)

М.П.

ПРИЛОЖЕНИЕ №3и
к Регламенту удостоверяющего центра СЗАО «Интерднестрком»
Для физических лиц и лиц, которым выдан специальный сертификат

Заявление
на возобновление действия сертификата открытого ключа электронной подписи

г. Тирасполь «___»_____202_ г.

Я, _____
(ФИО)

_____
(наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан)

прошу возобновить действие сертификата открытого ключа электронной подписи:
Данные Сертификата:

Идентификатор открытого ключа

_____
_____

Владелец сертификата:

_____
_____
_____
_____ /
(подпись) *(фамилия, имя, отчество)*

М.П.

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41

Уполномоченное лицо: _____ /
(подпись) *(фамилия, имя, отчество)*

М.П.

ПРИЛОЖЕНИЕ №3к
к Регламенту удостоверяющего центра СЗАО «Интерднестрком»

Для юридических лиц

Акт приема-передачи устройства
USB-токен

г. _____ «___»_____20__г.

Настоящим Актом подтверждается, что Удостоверяющий центр СЗАО «Интерднестрком», именуемый в дальнейшем **Удостоверяющий центр**,
в лице оператора Удостоверяющего центра, действующего на основании доверенности №__ от «__»_____ 2023 года **передал**,
а _____
(организационно-правовая форма и наименование юридического лица)

именуемый в дальнейшем «**Пользователь УЦ**»,
в лице _____
действующего на основании _____
(устава, доверенности № _____ от ___ ____ _____г.)

получил устройство USB-токен, в количестве _____ штук со следующими серийными номерами:

_____
_____
_____

Пользователь УЦ подтверждает, что корпус переданного Устройства не имеет видимых признаков повреждения и взлома.

Пользователь УЦ обязуется использовать и хранить токен в соответствии с Регламентом Удостоверяющего центра СЗАО «Интерднестрком», опубликованного на сайте http://ca.idc.md.

Пользователь УЦ согласен, что для начала использования токена необходимо осуществить действия в соответствии с Инструкцией пользователя для программы «IDC: Управление ключами», размещенной на сайте Удостоверяющего центра http://ca.idc.md.

Пользователь УЦ обязуется создать запрос на сертификат на АРМ Пользователя и произвести запись сертификата на токен.

Настоящий акт составлен в двух экземплярах, имеющих одинаковую юридическую силу.

От Удостоверяющего центра передал:	От Пользователя УЦ получил:
_____ /_____ Подпись расшифровка подписи	_____ /_____ Подпись расшифровка подписи
МП	МП

ПРИЛОЖЕНИЕ №3л
к Регламенту удостоверяющего центра СЗАО «Интерднестрком»
Для физических лиц и лиц, которым выдан специальный сертификат

Акт приема-передачи устройства
USB-токен

г. _____ «___»_____20__г.

Настоящим Актом подтверждается, что
Удостоверяющий центр СЗАО «Интерднестрком», именуемый в дальнейшем **Удостоверяющий центр**, в лице оператора Удостоверяющего центра, действующего на основании доверенности №__ от «__»_____ 2023 года **передал**,
а

_____
(фамилия, имя, отчество (при наличии) физического лица)

именуемый в дальнейшем «**Пользователь УЦ**», **получил** устройство USB-токен, в количестве _____штук со следующими серийными номерами:

_____
_____
_____

Пользователь УЦ подтверждает, что корпус переданного Устройства не имеет видимых признаков повреждения и взлома.

Пользователь УЦ обязуется использовать и хранить токен в соответствии с Регламентом Удостоверяющего центра СЗАО «Интерднестрком», опубликованного на сайте http://ca.idc.md.

Пользователь УЦ согласен, что для начала использования токена необходимо осуществить действия в соответствии с Инструкцией пользователя для программы «IDC: Управление ключами», размещенной на сайте Удостоверяющего центра http://ca.idc.md.

Пользователь УЦ обязуется создать запрос на сертификат на АРМ Пользователя и произвести запись сертификата на токен.

Настоящий акт составлен в двух экземплярах, имеющих одинаковую юридическую силу.

От Удостоверяющего центра передал:	Пользователь УЦ получил:
_____ /_____ Подпись расшифровка подписи	_____ /_____ Подпись расшифровка подписи
МП	МП

ПРИЛОЖЕНИЕ №3м
к Регламенту удостоверяющего центра СЗАО «Интерднестрком»

Заявление
на создание и выдачу сертификата открытого ключа электронной подписи №___

г. Тирасполь «___»_____202_ г.

Я, _____
(ФИО)

_____
(наименование документа удостоверяющего личность, серия, номер, дата выдачи, кем выдан)

прошу создать и выдать мне сертификат открытого ключа электронной подписи (далее – «Сертификат») со следующими данными:

Идентификатор открытого ключа: _____

Я заявляю, что любые действия, которые будут мной совершены на основании этого Сертификата, являются действиями, совершаемыми от моего имени.

Я понимаю и соглашаюсь с тем, что в случаях:

- обнаружения недостоверности сведений, указанных в настоящем Заявлении или в Сертификате;
- нарушения конфиденциальности закрытого ключа (компрометация закрытого ключа), также в иных случаях, установленных действующим законодательством Приднестровской Молдавской Республики и Регламентом Удостоверяющего центра СЗАО «Интерднестрком»,

выданный мне Сертификат может быть аннулирован Удостоверяющим центром СЗАО «Интерднестрком».

Заявитель:

/
_____
(подпись) (фамилия, имя, отчество)

Принято:
Удостоверяющий центр СЗАО «Интерднестрком»
Адрес: MD-3300. Г. Тирасполь, ул. Восстания, 41