РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ «ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ СЛУЖБА» КОМИТЕТА СВЯЗИ, ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИИ МИНИСТЕРСТВА ПО ИНВЕСТИЦИЯМ И РАЗВИТИЮ РЕСПУБЛИКИ КАЗАХСТАН

Утверждено приказом директора
РГП «ГТС» КСИИ МИР РК
от «__» февраля 2015 года
№ _____

ПРАВИЛА ПРИМЕНЕНИЯ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ПОДПИСЧИКОВ НАЦИОНАЛЬНОГО УДОСТОВЕРЯЮЩЕГО ЦЕНТРА РЕСПУБЛИКИ КАЗАХСТАН (CERTIFICATE PRACTICE STATEMENT)

Версия 1.0

2015 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Национальный удостоверяющий центр Республики Казахстан (далее — НУЦ РК) создан в целях предоставления физическим и юридическим лицам средств электронной цифровой подписи (далее — ЭЦП). Для этих целей НУЦ РК обеспечивает выдачу регистрационных свидетельств подписчикам НУЦ РК.

НУЦ РК осуществляет деятельность в соответствии со следующими законодательными и нормативно-правовыми актами Республики Казахстан, внутренними и публичными документами:

1) Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи»;

2) Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»;

3) Закон Республики Казахстан от 11 января 2007 года №217-III «Об информатизации»;

4) постановление Правительства Республики Казахстан от 24 февраля 2014 года №136 стандарт государственной услуги «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан» (далее – Стандарт);

5) приказ Министра транспорта и коммуникаций Республики Казахстан от 26 марта 2014 года № 209 «Об утверждении регламентов государственных услуг в области информатизации, оказываемых Министерством транспорта и коммуникаций Республики Казахстан»;

6) приказ Председателя Агентства Республики Казахстан по информатизации и связи от 8 декабря 2005 года №457-п «Об утверждении типового положения удостоверяющего центра Республики Казахстан»;

7) приказ Председателя Агентства Республики Казахстан по информатизации и связи от 8 декабря 2005 года №458-п «Об утверждении Правил выдачи, регистрации, хранения, отзыва регистрационных свидетельств, в том числе и на бумажном носителе и ведения регистра регистрационных свидетельств»;

8) приказ Министра связи и информации Республики Казахстан от 10 декабря 2010 года №348 «Об утверждении Правил деятельности корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов Республики Казахстан и Национального удостоверяющего центра Республики Казахстан»;

9) приказ Министра транспорта и коммуникаций Республики Казахстан от 26 марта 2014 года № 209 «О вопросах оказания Министерством транспорта и коммуникаций Республики Казахстан государственных услуг в сфере информатизации»;

10) СТ РК 1073-2007. Средства криптографической защиты информации. Общие требования;

11) рекомендуемый стандарт RFC 3647 Certificate Policy and Certification Practices Framework серии международных стандартов IETF (далее - RFC 3647);

12) Серия рекомендуемых стандартов ITU-T X.500;

13) рекомендуемый стандарт RFC 5280 Certificate and Certificate Revocation List Profile (далее - RFC 5280);

14) регламент взаимодействия Республиканского государственного предприятия на праве хозяйственного ведения «Государственная техническая служба» Комитета связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан и Республиканского государственного предприятия на праве хозяйственного ведения «Центр обслуживания населения» Министерства по инвестициям и развитию Республики Казахстан по оказанию государственной услуги «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан»_____.

15) политика применения регистрационных свидетельств подписчиков НУЦ РК (Certificate Policy)____.

НУЦ РК выдаёт регистрационные свидетельства следующих видов:

регистрационное свидетельство для физических лиц (для подписи и аутентификации);

регистрационное свидетельство для юридических лиц (для подписи и аутентификации);

регистрационное свидетельство для нерезидентов (для подписи и аутентификации);

регистрационные свидетельства SSL;

регистрационные свидетельства для пользователей системы Казначейство-Клиент (для подписи и аутентификации).

1.1. ПОНЯТИЯ И АББРЕВИАТУРЫ

В настоящих Правилах используются следующие понятия и аббревиатуры:

1) активы – ресурсы РГП ГТС направленные на обеспечения непрерывности работы НУЦ РК.

2) бизнес-идентификационный номер (далее – БИН) - уникальный номер формируемый для юридического лица (филиала и представительства) и индивидуального предпринимателя, осуществляющего деятельность в виде совместного предпринимательства;

3) внутренняя контрольная среда – совокупность контролей процессов НУЦ РК;

4) государственная услуга – государственная услуга «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан»;

5) журнал - файл с записями о событиях ИС НУЦ РК в хронологическом порядке

6) заявитель - физическое или юридическое лицо (филиал/представительство) подавшее документы на выдачу или на отзыв (аннулирование) регистрационного свидетельства до момента регистрации регистрационного свидетельства или признания регистрационного свидетельства недействительным (аннулированным);

7) закрытый ключ ЭЦП — последовательность электронных цифровых символов, известная подписчику НУЦ РК и предназначенная для создания электронной цифровой подписи с использованием средств ЭЦП;

8) инфраструктура открытых ключей (далее - ИОК) — комплекс информационных систем, организационных и технических мероприятий, направленный на управление регистрационными свидетельствами в соответствии с законодательством Республики Казахстан об электронном документе и электронной цифровой подписи;

9) индивидуальный идентификационный номер (далее – ИИН) - уникальный номер, формируемый для физического лица, в том числе индивидуального предпринимателя, осуществляющего деятельность в виде личного предпринимательства;

10) интернет-ресурс НУЦ РК – интернет-ресурс НУЦ РК www.pki.gov.kz;

11) национальный удостоверяющий центр Республики Казахстан (далее – НУЦ РК) — удостоверяющий центр, обслуживающий участников «электронного правительства», государственных и негосударственных информационных систем;

12) ключевая пара - набор, состоящий из двух ключей: закрытого (секретного) ключа и открытого ключа;

13) корневой удостоверяющий центр Республики Казахстан (далее КУЦ РК) – удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров;

14) КСИИ МИР РК - республиканское государственное учреждение «Комитет связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан»;

15) открытый ключ ЭЦП - последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности ЭЦП в электронном документе;

16) пользовательское соглашение - пользовательское соглашение интернет-ресурса www.pki.gov.kz для получения государственной услуги «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан», утверждённое Приказом Директора РГП «ГТС» №01-06/39 от 4 апреля 2014 года и опубликованное на интернет-ресурсе www.pki.gov.kz;

17) перечень персональных данных - перечень персональных данных, необходимых и достаточных для выполнения осуществляемых задач по государственной услуге «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан», утверждённый Приказом Директора РГП «ГТС» №01-06/39 от 4 апреля 2014 года и опубликованный на интернет-ресурсе НУЦ РК www.pki.gov.kz;

18) портал – веб-портал электронного правительства Республики Казахстан e-gov;

19) регистрационное свидетельство - документ на бумажном носителе или электронный документ, выдаваемый НУЦ РК для подтверждения соответствия электронной цифровой подписи требованиям, установленным нормативно-правовыми актами Республики Казахстан;

20) РГП ГТС - Республиканское государственное предприятие на праве хозяйственного ведения «Государственная техническая служба» Комитета связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан;

21) РГП ЦОН - Республиканского государственного предприятия на праве хозяйственного ведения «Центр обслуживания населения» Министерства по инвестициям и развитию Республики Казахстан;

22) список отозванных регистрационных свидетельств (далее – СОРС) - перечень всех регистрационных свидетельств подписчиков НУЦ РК, отозванных на момент выпуска СОРС;

23) средства ЭЦП - совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи;

24) электронно-цифровая подпись (далее – ЭЦП) - набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания;

25) WebTrust - международный стандарт «Принципы и критерии услуг в области доверия для удостоверяющих центров», версия 2.0 («Trust Service Principles and Criteria for Certification Authorities Version 2.0»);

26) DN-имя - уникальное имя, присваиваемое подписчику НУЦ РК и содержащееся в его регистрационном свидетельстве подписчика НУЦ РК;

27) OSCP (проверка статуса регистрационного свидетельства) - данный метод проверки подтверждает, отозвано ли проверяемое регистрационное свидетельство на момент отправки запроса (текущее время);

28) TSP - сервис штампа времени.

1.2. ОБЗОР

Настоящие Правила применения регистрационных свидетельств подписчиков НУЦ РК (Certificate practice statement) (далее — Правила) определяет деятельность НУЦ РК в отношении услуг, связанных с жизненным циклом регистрационных свидетельств НУЦ РК и подписчиков НУЦ РК, и применимы ко всем участникам ИОК НУЦ РК, которые используют регистрационные свидетельства подписчики НУЦ РК, выпущенные НУЦ РК.

Настоящие Правила составлены в соответствии со следующими рекомендуемыми стандартами:

принципы и критерии международного стандарта WebTrust для удостоверяющих центров, версия 2.0 (Trust Services Principle and Criteria for Certification Authorities, version 2.0);

рекомендации руководства по разработке политик применения регистрационных свидетельств и инструкций по применению регистрационных свидетельств инфраструктуры открытых ключей в соответствии с международным стандартом RFC 3647 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework». В соответствии с вышеуказанными стандартами, настоящие Правила состоят из 9 глав, которые описывают практики предоставления услуг в отношении регистрационных свидетельств подписчиков НУЦ РК, а также контроли безопасности, применяемые для защиты ИОК НУЦ РК. В целях сохранения соответствия структуры Правил принципы и критерии международного стандарта WebTrust и рекомендациям RFC 3647не применимые к практикам ИОК НУЦ РК, содержат пометку «не применимо» или «не оговаривается».

Настоящие Правила описывают деятельность НУЦ РК, применяемые в отношении регистрационных свидетельств подписчиков НУЦ РК в соответствии требованиями, установленными в Политике применения регистрационных свидетельств подписчиков НУЦ РК (Certificate policy). Деятельность НУЦ РК соответствуют требованиям следующих стандартов, актуальных на момент публикации Правил:

принципы и критерии международного стандарта WebTrust для удостоверяющих центров, версия 2.0 (Trust Services Principle and Criteria for Certification Authorities, version 2.0);

базовые требования к выпуску и управлению публичными регистрационными свидетельствами, версия 1.1.9 (Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, version 1.1.9).

1.3. НАИМЕНОВАНИЕ И ИДЕНТИФИКАЦИЯ ДОКУМЕНТА

Наименование настоящего документа: Правила применения регистрационных свидетельств подписчиков Национального

удостоверяющего центра Республики Казахстан (Certificate practice statement).

Версия документа: 1.0.

Введены в действие приказом директора РГП ГТС№___ от ___ февраля 2015 года.

Действующая версия настоящих Правил публикуется на интернет-ресурсе НУЦ РК.

1.4. УЧАСТНИКИ ИОК НУЦ РК

1.4.1. НУЦ РК

НУЦ РК является удостоверяющим центром, который выдаёт регистрационные свидетельства НУЦ РК, предназначенные для использования в соответствии с положениями пунктом **Ошибка! Источник ссылки не найден.** настоящих Правил. В ИОК НУЦ РК не допускаются иные удостоверяющие центры.

НУЦ РК осуществляет деятельность, которая непосредственно связана с ИОК, а именно:

получение и обработка запросов на выдачу и отзыв регистрационных свидетельств НУЦ РК;

выдача и отзыв регистрационных свидетельств НУЦ РК;

публикация и поддержка CORC и промежуточных списков отозванных регистрационных свидетельств НУЦ РК (далее — Дельта CORC);

обработка запросов службы OCSP:

обработка запросов службы TSP.

1.4.2. Центры регистрации

В ИОК НУЦ РК функцию центров регистрации (далее — ЦР) выполняют филиалы РГП ЦОН и структурное подразделение РГП ГТС. Взаимодействие РГП ЦОН и РГП ГТС осуществляется на основе Регламента взаимодействия РГП ГТС и РГП ЦОН по оказанию государственной услуги «Выдача и отзыв регистрационного свидетельства НУЦ РК».

Функции ЦР:

1) оператор ЦОН осуществляет:

запись регистрационных свидетельств на удостоверение личности заявителя, содержащее электронный носитель информации (чип);

проверку (идентификацию) личности заявителя и проверку предоставленных документов;

подтверждение электронного запроса заявителя путем удостоверения его своей ЭЦП в случае успешной проверки (идентификации) личности заявителя и соответствия предоставленных им документов, а также отправку электронного запроса в информационную систему;

выдачу заявителю расписки о приеме документов;

отзыв регистрационных свидетельств с удостоверения личности подписчика НУЦ РК;

заполнение формы электронного запроса для отзыва регистрационного свидетельства и подтверждает электронный запрос путем удостоверения его своей ЭЦП, а также отправка его в информационную систему;

2) ведущий специалист или главный специалист РГП ГТС осуществляет:

проверку (идентификацию) личности заявителя и соответствие его заявления на бумажном носителе с заявлением, поступившим на Портал;

подтверждение электронного запроса заявителя на Портале путем удостоверения ЭЦП ведущего специалиста или главного специалиста РГП ГТС и отправка его в информационную систему;

заполнение формы электронного запроса для отзыва регистрационного свидетельства и подтверждает электронный запрос путем удостоверения его своей ЭЦП, а также отправка его в информационную систему;

запись регистрационных свидетельств на удостоверение личности подписчика НУЦ РК;

отзыв регистрационных свидетельств с удостоверения личности подписчика НУЦ РК.

1.4.3. Подписчики НУЦ РК

Подписчик НУЦ РК — владелец регистрационного свидетельства, физическое или юридическое лицо, на имя которого выдано регистрационное свидетельство, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве.

1.4.4. Доверяющие стороны

Доверяющая сторона — субъект, который предпринимает действия, основываясь на регистрационном свидетельстве, выпущенном НУЦ РК. Зависимая сторона может быть подписчиком НУЦ РК.

1.4.5. Другие участники

Не применимо.

1.5. ИСПОЛЬЗОВАНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

1.5.1. Разрешённые способы использования регистрационных свидетельств подписчиков НУЦ РК

Регистрационные свидетельства подписчиков НУЦ РК применимы для следующих целей:

1) подписание электронных документов электронной цифровой подписью;
2) проверка электронной цифровой подписи;

3) аутентификация подписчиков НУЦ РК в государственных и негосударственных информационных системах Республики Казахстан;

4) защита канала передачи информации между пользователем и интернет-ресурсом (SSL).

1.5.2. Запрещённые способы использования регистрационных свидетельств подписчиков НУЦ РК

Способы использования регистрационных свидетельств подписчиков НУЦ РК не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящих Правил.

Подписчикам НУЦ РК и информационным системам запрещается использование регистрационных свидетельств НУЦ РК в случаях:

1) после окончания срока действия регистрационного свидетельства подписчика НУЦ РК;
2) в случае отзыва регистрационного свидетельства подписчика НУЦ РК;
3) в случае подозрения на компрометацию закрытого ключа, удостоверенного регистрационным свидетельством подписчика НУЦ РК;
4) в случае обнаруженной компрометации закрытого ключа, удостоверенного регистрационным свидетельством подписчика НУЦ РК;
5) в случаях, не относящихся к разрешённым способам использования регистрационных свидетельств подписчиков НУЦ РК.

1.6. УПРАВЛЕНИЕ НАСТОЯЩИМИ ПРАВИЛАМИ

Разработка, поддержка и обновление настоящих Правил осуществляется РГП ГТС.

Реквизиты:

юридический адрес: Республика Казахстан, 010000, г. Астана, ул. Жирентаева, дом 1/1;

фактический адрес: Республика Казахстан, 010000, г. Астана, ул. Күйші Дина, дом 16;

электронный адрес РГП ГТС: info@pki.gov.kz;

телефон 55 99 99 (внутренний 399).

Изменения или дополнения в настоящие Правила вносятся после их проверки на соответствие Политике применения регистрационных свидетельств подписчиков НУЦ РК (Certificate Policy). Предложения по изменениям или дополнениям в Правила вносятся ответственными работниками РГП ГТС и утверждаются приказом директора РГП ГТС или уполномоченным заместителем.

Утверждённые изменённые или дополненные Правила публикуются на интернет-ресурсе НУЦ РК в виде отдельного документа, содержащего полный текст Правил, или уведомления о внесении изменений и самих изменений с указанием последовательного увеличивающегося номера версии Правил. Все устаревшие версии Правил также остаются опубликованными на интернет-ресурсе НУЦ РК. Все устаревшие версии Правил снабжаются пометкой с указанием диапазона дат действительной силы версии Правил и ссылкой на действующую версию Правил.

2. ОТВЕТСТВЕННОСТЬ В ОТНОШЕНИИ ПУБЛИКАЦИИ И ХРАНЕНИЯ

2.1. ХРАНЕНИЕ И ДОСТУПНОСТЬ ПУБЛИЧНОЙ ИНФОРМАЦИИ

НУЦ РК обеспечивает публичную доступность 24 часа в сутки, 7 дней в неделю следующих материалов на интернет-ресурсе НУЦ РК:

корневые регистрационные свидетельства КУЦ РК, доступные по следующим ссылкам: http://root.gov.kz/cert/root_rsa.cer (RSA) и http://root.gov.kz/cert/root_gost.cer (ГОСТ).

СОРС;

Дельта СОРС;

службы OCSP доступная по ссылке http://ocsp.pki.gov.kz;

служба TSP, доступная по ссылке http://tsp.pki.gov.kz;

Политика применения регистрационных свидетельств подписчика НУЦ РК (Certificate Policy);

настоящие Правила;

пользовательское соглашение.

2.2. ПУБЛИКАЦИЯ ИНФОРМАЦИИ О РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВАХ ПОДПИСЧИКОВ НУЦ РК

2.2.1. СОРС НУЦ РК

СОРС НУЦ РК предоставляется в электронной форме и формате, определённом рекомендациями RFC 5280 и настоящими Правилами. НУЦ РК публикует следующие виды СОРС:

1) СОРС для регистрационных свидетельств на алгоритме RSA, доступные по адресам:

http://crl.pki.gov.kz/rsa.crl —СОРС для регистрационных свидетельств RSA;

http://crl1.pki.gov.kz/rsa.crl — резервный СОРС для регистрационных свидетельств RSA;

http://crl.pki.gov.kz/d_rsa.crl — дельта СОРС для регистрационных свидетельств RSA;

http://crl1.pki.gov.kz/d_rsa.crl— резервный дельта СОРС для регистрационных свидетельств RSA;

2) СОРС для регистрационных свидетельств на алгоритме ГОСТ, доступные по адресам:

http://crl.pki.gov.kz/gost.crl —СОРС для регистрационных свидетельств ГОСТ;

http://crl1.pki.gov.kz/gost.crl - резервный СОРС для регистрационных свидетельств ГОСТ;
http://crl.pki.gov.kz/d_gost.crl — дельта СОРС для регистрационных свидетельств ГОСТ;
http://crl1.pki.gov.kz/d_gost.crl — резервный дельта СОРС для регистрационных свидетельств ГОСТ.

2.2.2. Служба OCSP НУЦ РК

НУЦ РК также предоставляет службу анонимной проверки статуса регистрационного свидетельства подписчика НУЦ РК посредством службы OCSP, доступной по ссылке http://ocsp.pki.gov.kz.

2.3. ПЕРИОД ПУБЛИКАЦИИ ИНФОРМАЦИИ

СОРС публикуется раз в сутки. Срок действия СОРС составляет 25 часов.

НУЦ РК также публикует обновления СОРС в виде отдельного Дельта СОРС, содержащего перечень регистрационных свидетельств подписчиков НУЦ РК, отозванных с момента выпуска последнего СОРС. Дельта СОРС формируется не реже чем каждые 2 часа и действует до выпуска следующего Дельта СОРС, но не более чем в течение 3 часов с момента своей публикации.

2.4. КОНТРОЛЬ ДОСТУПА К ПУБЛИЧНОЙ ИНФОРМАЦИИ

В НУЦ РК реализованы меры информационной и физической безопасности с целью предотвращения несанкционированного внесения, изменения или удаления информации, содержащейся в СОРС и информационной системе НУЦ РК.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. ПРИСВАИВАНИЕ ИМЁН

3.1.1. Типы имён, присваиваемых подписчику НУЦ РК

Регистрационное свидетельство подписчика НУЦ РК содержат отличительные имена в DN-имени в формате рекомендованный стандартом X.501 «Information technology - Open Systems Interconnection - The Directory: Models» из серии рекомендуемых стандартов ITU-T X.500 в поле «Subject», состоящие из следующих компонентов и указанных в пунктах 7.1.1.-7.1.9.:

Компонент	Значение	Длина	Обязательность
Наименование страны «countryName»	KZ	2 символа	Обязательное
Административно-территориальная единица «State»	Область, город республиканского значения, в котором находится заявитель	Не более 32 символов	Обязательное
Местонахождение «Locality»	Город, в котором находится заявитель	Не более 16 символов	Обязательное
Адрес электронной почты (Email)	Адрес электронной почты заявителя	Не более 32 символов	Обязательное
Персональное имя «commonName»	Фамилия и имя заявителя	Не более 64 символов	Обязательное
Серийный номер «serialNumber»	ИИН заявителя	15 символов	Обязательное
Отчество «givenName»	Отчество заявителя	Не более 32 символов	Необязательное

3.1.2. Необходимость использования персональных данных в DN-имени

НУЦ РК выдаёт регистрационные свидетельства подписчиков НУЦ РК, которые содержат персональные данные в DN-имени, позволяющие идентифицировать подписчика НУЦ РК и область применения регистрационного свидетельства подписчика НУЦ РК.

3.1.3. Анонимность или использование псевдонимов подписчиками НУЦ РК

Анонимность и использование псевдонимов подписчиками НУЦ РК не допускается.

3.1.4. Правила интерпретации DN-имён

Отличительные DN-имена должны включать все элементы, указанные в соответствующем профиле регистрационного свидетельства подписчика НУЦ РК согласно спецификации стандарта X.509 из серии рекомендуемых стандартов ITU-T X.500 и RFC-5280. НУЦ РК заполняет поле «Subject» персональными данными подписчика НУЦ РК, полученными из государственной базы данных физических лиц и государственной базы данных юридических лиц на основании предоставленных заявителем идентифицирующих данных.

3.1.5. Использование уникальных DN-имён

Каждому уникальному подписчику НУЦ РК должно соответствовать уникальное имя в поле «Subject» регистрационного свидетельства подписчика НУЦ РК указанных в пункте 3.1.1. настоящих Правил.

3.1.6. Распознавание, аутентификация и роль торговых марок

В отличительных полях «Subject» и «Issuer» регистрационных свидетельств НУЦ РК разрешено использовать только официально зарегистрированные названия юридических лиц. НУЦ РК не допускает использование торговых марок в отличительных полях «Subject» и «Issuer» регистрационных свидетельств.

Использование подписчиками НУЦ РК в отличительном поле «Subject»торговых марок в наименовании юридических лиц осуществляется в соответствии с действующим законодательством Республики Казахстан.

3.2. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ЗАЯВИТЕЛЕЙ ПРИ ВЫДАЧЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

Подтверждение принадлежности и действительности открытого ключа ЭЦП ЦР осуществляется на основании заявления на выдачу регистрационных свидетельств НУЦ РК заявителя, оформленного посредством Портала, и состоит из следующих этапов:

1) заявитель в течение 15 минут выбирает соответствующую услугу на Портале, заполняет формы запроса для получения регистрационных свидетельств и направляет запрос через шлюз «электронного правительства» (далее – ШЭП) в Государственную базы данных «Физические лица» и «Юридические лица» (далее – государственные базы данных);

2) в случае наличия данных о заявителе в государственных базах данных, через Портал в течение 5 минут выводит сообщение заявителю о наличии данных о заявителе и обеспечивает дальнейшее продолжение заполнение форм запросов на Портале;

3) информационная система НУЦ РК генерирует ключевую пару заявителя;

4) заявителю в течение 5 минут после заполнения форм запросов на Портале и регистрации электронного запроса в информационной системе, на адрес электронной почты заявителя поступает заявление с уникальным номером для дальнейшего его предоставления в ЦР;

5)заявитель предоставляет в ЦР заявление и соответствующие документы;

6) ЦР течение 15 минут для физических лиц и в течение 20 минут для юридических лиц с момента сдачи заявителем необходимых документов, осуществляет проверку (идентификацию) личности заявителя и проверку предоставленных документов в соответствии с пунктами 3.2.2. – 3.2.9. настоящих Правил;

7) в случае успешной проверки (идентификации) личности заявителя и соответствия предоставленных документов, оператор ЦР обеспечивает подтверждение электронного запроса заявителя путем удостоверения его своей ЭЦП, отправляет его в информационную систему и выдает заявителю расписку о приеме документов;

8) после подтверждения ЦР запроса на выдачу регистрационных свидетельств НУЦ РК заявитель получает уведомление об успешном выпуске регистрационных свидетельств со ссылкой для их установки.

ЦР обеспечивает заявителю возможность записи регистрационных свидетельств НУЦ РК на удостоверение личности заявителя, содержащее электронный носитель информации (чип):

1) заявитель в течение 20 минут предоставляет в ЦР свое удостоверение личности, содержащее электронный носитель информации (чип);

2) ЦР в течение 20 минут с момента получения от заявителя его удостоверения личности, осуществляет проверку (идентификацию) личности заявителя. В случае наличия данных об заявителя в государственных базах данных, государственные базы данных в течение 5 минут выводят сообщение оператору ЦР о наличии данных о заявителе и обеспечивают дальнейшее продолжение заполнение форм запросов;

3) заявитель в течение 1 минуты вводит пин-код от своего удостоверения личности.

В случае корректного ввода пин-кода, оператор ЦР регистрирует электронный запрос в информационной системе, распечатывает его для подписания заявителем.

Оператор ЦР обеспечивает подтверждение электронного запроса заявителем путем удостоверения его своей ЭЦП и отправляет его в информационную систему.

3.2.1. Представление интересов заявителя третьим лицом

Допускается представление интересов заявителя третьим лицом при подачи документов заявителя в ЦР на основании доверенности на разовое получение или отзыв регистрационных свидетельств НУЦ РК (нотариально удостоверенной), установленной формы согласно приложения 2 и приложения 5 к Стандарту.

3.2.2. Проверка (идентификация) заявителя (физическое лицо)

Сведения, указанные в заявлении физического лица на выдачу регистрационных свидетельств, подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР и представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств НУЦ РК (от физического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (физического лица) при представлении интересов заявителя третьим лицом в соответствии с пунктом 3.2.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность заявителя (физического лица) или его представителя.

3.2.3. Проверка (идентификация) заявителя (физическое лица - нерезидента)

Сведения, указанные в заявлении на выдачу регистрационных свидетельств НУЦ РК (от физического лица) на выдачу регистрационных свидетельств, подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР и представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств НУЦ РК (от физического лица), полученное с Портала и содержащее

уникальный номер;

2) доверенность на разовое получение или отзыв регистрационных свидетельств НУЦ РК для физических лиц при представлении интересов заявителя третьим лицом в соответствии с пунктом 3.2.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность заявителя (физического лица - нерезидента) или его представителя;

4) один из нижеперечисленных документов, содержащий ИИН и подтверждающий, что данный заявитель (физическое лицо нерезидент) зарегистрирован на территории Республики Казахстан:

вид на жительство иностранца в Республике Казахстан;

удостоверение лица без гражданства;

регистрационное свидетельство для иностранцев.

3.2.4. Проверка (идентификация) заявителя (юридическое лицо)

Сведения, указанные в заявлении на выдачу регистрационных свидетельств НУЦ РК (от юридического лица) подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР и представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств НУЦ РК (от юридического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (юридического лица) в соответствии с пунктом 3.2.1. настоящих Правил; для первого руководителя юридического лица или лица, исполняющего его обязанности, вместо доверенности представляется справка с места работы либо заверенная печатью юридического лица копия приказа (решения, протокола) о назначении на должность первого руководителя или лица, исполняющего его обязанности;

3) оригиналы документов, удостоверяющих личность заявителя либо представителя заявителя (юридического лица);

4) справку о государственной регистрации (перерегистрации) юридического лица заявителя в качестве юридического лица (либо копию, нотариально засвидетельствованную в случае непредставления оригиналов) – для юридического лица.

3.2.5. Проверка (идентификация) заявителя (юридическое лицо – нерезидент)

Сведения, указанные в заявлении юридического лица нерезидента на выдачу регистрационных свидетельств, подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств НУЦ РК (от юридического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (юридического лица - нерезидента) в соответствии с пунктом 3.2.1 настоящих Правил;

3) оригиналы документов, удостоверяющих личность представителя заявителя (юридического лица нерезидента);

4) один из нижеперечисленных документов, содержащий индивидуальный идентификационный номер и подтверждающий, что данный представитель юридического лица-нерезидента зарегистрирован на территории Республики Казахстан:

вид на жительство иностранца в Республике Казахстан;

удостоверение лица без гражданства;

регистрационное свидетельство для иностранцев;

5) один из нижеперечисленных документов, содержащий БИН и подтверждающий, что данное юридическое лицо-нерезидент зарегистрировано на территории Республики Казахстан Министерством юстиции Республики Казахстан:

справку об учётной регистрации (перерегистрации) филиала, представительства – для юридических лиц-нерезидентов, осуществляющих деятельность в Республике Казахстан через филиалы и представительства (с образованием постоянного учреждения) или свидетельство о государственной (учетной) регистрации (перерегистрации) юридического лица (филиала, представительства выданное до введения в действие Закона Республики Казахстан от 17 апреля 1995 года «О государственной регистрации юридических лиц и учетной регистрации филиалов и представительств», является действительным до прекращения деятельности юридического лица;

регистрационное свидетельство для юридических лиц-нерезидентов;

владеющих в Республике Казахстан объектами налогообложения;

являющихся дипломатическими и приравненными к ним представительствами иностранного государства, аккредитованными в Республике Казахстан;

осуществляющих деятельность через постоянное учреждение без открытия филиала, представительства;

открывающих текущие счета в банках-резидентах.

3.2.6. Проверка (идентификация) заявителя (участник информационной системы «Казначейство-клиент»)

Сведения, указанные в заявлении на выдачу регистрационного свидетельства для участников информационной системы «Казначейство-клиент», подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств НУЦ РК (от юридического лица для пользователей информационной системы «Казначейство-Клиент»), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (участника информационной системы «Казначейство-клиент») в соответствии с пунктом 3.2.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность заявителя либо представителя заявителя (участника информационной системы «Казначейство-клиент»);

4) соглашение либо дополнительное соглашение об использовании ЭЦП между Комитетом казначейства Республики Казахстан и заявителем (участником информационной системы «Казначейство-клиент»).

3.2.7. Проверка (идентификация) заявителя (физическое лицо - владелец доменного имени интернет - ресурса)

Сведения, указанные в заявлении на выдачу SSL регистрационного свидетельства для физических лиц владельцев доменного имени интернет-ресурса, подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР представлением следующих документов:

1) заявление на выдачу SSL регистрационного свидетельства НУЦ РК (от физического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (физического лица владельца доменного имени интернет-ресурса) при представлении интересов заявителя третьим лицом в соответствии с пунктом 3.2.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность заявителя (физического лица владельца доменного имени интернет-ресурса) или его представителя;

4) один из нижеперечисленных подтверждающих документов на право владения доменным именем интернет-ресурса:

сертификат о владении доменным именем;

справка от регистратора домена;

копию договора о регистрации доменного имени;

публичная оферта о регистрации доменного имени;

другой подтверждающий документ.

3.2.8. Проверка (идентификация) заявителя (юридическое лицо - владелец доменного имени интернет-ресурса)

Сведения, указанные в заявлении на выдачу SSL регистрационного свидетельства для юридических лиц владельцев доменного имени интернет-ресурса, подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР представлением следующих документов:

1) заявление на выдачу SSL регистрационного свидетельства НУЦ РК (от юридического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (юридического лица владельца доменного имени интернет-ресурса) в соответствии с пунктом 3.2.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность представителя заявителя (юридического лица владельца доменного имени интернет-ресурса);

4) один из нижеперечисленных подтверждающих документов на право владения доменным именем интернет-ресурса:

сертификат о владении доменным именем;

справка от регистратора домена;

копию договора о регистрации доменного имени;

публичную оферту о регистрации доменного имени;

другой подтверждающий документ.

3.2.9. Проверка (идентификация) заявителя (участник системы Е-нотариат)

Сведения, указанные в заявлении на выдачу регистрационного свидетельства для участника информационной системы «Е-нотариат», подтверждаются при личном прибытии заявителя либо представителя заявителя в ЦР представлением следующих документов:

1) заявление на выдачу регистрационных свидетельств, полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя заявителя (участника информационной системы «Е-нотариат») при представлении интересов заявителя третьим лицом в соответствии с п. 3.2.1 настоящей Политики;

3) оригиналы документов, удостоверяющих личность заявителя (участник информационной системы «Е-нотариат»);

4) справку с места работы:

для нотариусов — выданную территориальной нотариальной палатой;

для сотрудников Министерства юстиции Республики Казахстан, территориальных органов юстиции, Республиканской нотариальной палаты, территориальных нотариальных палат — с указанием должности).

3.3. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ЗАЯВИТЕЛЯ ПРИ ПОВТОРНОМ ПОЛУЧЕНИИ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

НУЦ РК не предоставляет возможности повторного получения регистрационных свидетельств подписчика НУЦ РК, идентичных выпущенным ранее регистрационным свидетельствам НУЦ РК при утрате или их повреждения.

НУЦ РК также не допускает замену ключевых пар подписчиков НУЦ РК в действующих регистрационных свидетельствах без повторного получения регистрационного свидетельства НУЦ РК.

Повторное получение регистрационных свидетельств заявителем осуществляется до истечения срока действия регистрационного свидетельства подписчика НУЦ РК:

1) заявитель в течение 15 минут выбирает соответствующую услугу на Портале, производит вход в личный кабинет при помощи своего действующего регистрационного свидетельства подписчика НУЦ РК, заполняет формы запроса для получения регистрационных свидетельств и направляет запрос через шлюз в государственные базы данных;

2) в случае наличия данных о заявителе в государственных базах данных, государственные базы данных через Портал в течение 5 минут выводят сообщение заявителю о наличии данных о заявителе и обеспечивают дальнейшее продолжение заполнение форм запросов на Портале;

3) заявитель в течение 1 дня после заполнения форм запросов на Портале и регистрации электронного запроса в информационной системе, получает уведомление об успешном выпуске регистрационных свидетельств со ссылкой для их установки;

В случае выдачи регистрационных свидетельств после отзыва существовавших регистрационных свидетельств НУЦ РК, подписчик НУЦ РК проходит проверку (идентификацию) личности заявителя в соответствии с процедурой, описанной в пункте 3.2. настоящих Правил.

3.4. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ПОДПИСЧИКА НУЦ РК ПРИ ОТЗЫВЕ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ

При отзыве регистрационных свидетельств подписчик НУЦ РК:

1) в случае отзыва регистрационного свидетельства через Портал

подписчик НУЦ РК в течение 15 минут выбирает соответствующую услугу на Портале, производит вход в личный кабинет при помощи своего действующего регистрационного свидетельства заполняет формы запроса для отзыва регистрационных свидетельств и направляет электронный запрос, подписанный ЭЦП подписчика НУЦ РК через Портал в информационную систему.

2) в случае отзыва через ЦР:

подписчик НУЦ РК предоставляет в ЦОН заявление;

оператор ЦР в течение 20 минут с момента сдачи подписчиком НУЦ РК необходимых документов, осуществляет проверку (идентификацию) личности подписчика НУЦ РК и проверку предоставленных документов в соответствии с пунктами 3.4. 2. - 3.4.9. настоящих Правил;

в случае успешной проверки (идентификации) личности подписчика НУЦ РК и соответствия предоставленных документов, оператор ЦР подтверждает электронное заявление на отзыв регистрационного свидетельства подписчика НУЦ РК путём удостоверения его своей ЭЦП, отправляет его в информационную систему и выдаёт заявителю расписку о приёме документов.

3.4.1. Представление интересов подписчика НУЦ РК третьим лицом

Допускается представление интересов заявителя третьим лицом при подачи документов подписчика НУЦ РК в ЦР на основании доверенности на разовое получение или отзыв регистрационных свидетельств НУЦ РК (нотариально удостоверенной), установленной формы согласно приложения 2 и приложения 5 к Стандарту.

3.4.2. Проверка (идентификация) подписчика НУЦ РК (физическое лицо)

Сведения, указанные в заявлении физического лица на отзыв регистрационных свидетельств, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР представлением следующих документов:

1) заявление на отзыв регистрационных свидетельств НУЦ РК (от физического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя подписчика НУЦ РК (физического лица) при представлении интересов подписчика НУЦ РК третьим лицом в соответствии с пунктом 3.4.1. настоящих Правил.

3) оригиналы документов, удостоверяющих личность подписчика НУЦ РК (физического лица) или его представителя.

3.4.3. Проверка (идентификация) подписчика НУЦ РК (физические лица - нерезиденты)

Сведения, указанные в заявлении физического лица на отзыв регистрационного свидетельства, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР представлением следующих документов:

1) заявление на отзыв регистрационных свидетельств НУЦ РК (от физического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя подписчика НУЦ РК (физического лица нерезидента) при представлении интересов подписчика НУЦ РК третьим лицом в соответствии с пунктом 3.4.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность подписчика НУЦ РК (физического лица нерезидента) или его представителя.

3.4.4. Проверка (идентификация)подписчика НУЦ РК (юридическое лицо)

Сведения, указанные в заявлении юридического лица на отзыв регистрационных свидетельств, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР представлением следующих документов:

1) заявление на отзыв регистрационных свидетельств НУЦ РК (от юридического лица), полученное с Портала, содержащее уникальный номер и заверенное печатью юридического лица, либо выписку из приказа об увольнении заявителя. В случае представления выписки из приказа об увольнении, подпись руководителя и печать организации не требуется;

2) оригиналы документов, удостоверяющих личность представителя подписчика НУЦ РК (юридического лица) в соответствии с пунктом 3.4.1 настоящей Политики.

3.4.5. Проверка (идентификация)подписчика НУЦ РК (юридическое лицо – нерезидент)

Сведения, указанные в заявлении юридического лица нерезидента на отзыв регистрационных свидетельств, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР представлением следующих документов:

1) заявление на отзыв регистрационных свидетельств НУЦ РК (от юридического лица), полученное с Портала, содержащее уникальный номер и заверенное печатью юридического лица, либо выписку из приказа об увольнении заявителя. В случае представления выписки из приказа об увольнении, подпись руководителя и печать организации не требуются;

2) оригиналы документов, удостоверяющих личность представителя подписчика НУЦ РК (юридического лица нерезидента).

3.4.6. Проверка (идентификация) подписчика НУЦ РК (участник информационной системы «Казначейство-клиент»)

Сведения, указанные в заявлении на отзыв регистрационных свидетельств для пользователей информационной системы «Казначейство-клиент», подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР

представлением следующих документов:

1) заявление на отзыв регистрационных свидетельств НУЦ РК (от юридического лица для пользователей информационной системы «Казначейство-Клиент»), полученное с Портала, содержащее уникальный номер и заверенное печатью юридического лица, либо выписку из приказа об увольнении заявителя. В случае представления выписки из приказа об увольнении, подпись руководителя и печать организации не требуются;

2) доверенность на представителя подписчика НУЦ РК (участника информационной системы «Казначейство-клиент») при представлении интересов подписчика НУЦ РК третьим лицом в соответствии с пунктом 3.4.1. настоящих Правил;

3) оригиналы документов, удостоверяющих личность представителя подписчика НУЦ РК НУЦ РК (участника информационной системы «Казначейство-клиент»).

3.4.7. Проверка (идентификация) подписчика НУЦ РК (физическое лицо владельцев доменного имени интернет-ресурса)

Сведения, указанные в заявлении на отзыв регистрационного свидетельства SSL для физического лица владельца доменного имени интернет-ресурса, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК в ЦР представлением следующих документов:

1) заявление на отзыв SSL регистрационного свидетельства НУЦ РК (от физического лица), полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя подписчика НУЦ РК (физическое лицо владелец доменного имени Интернет-ресурса) при представлении интересов заявителя третьим лицом в соответствии с пунктом 3.4.1 настоящих Правил;

3) оригиналы документов, удостоверяющих личность подписчика НУЦ РК (физическое лицо владелец доменного имени интернет-ресурса).

3.4.8. Проверка (идентификация) подписчика НУЦ РК (юридическое лицо владелец доменного имени интернет-ресурса)

Сведения, указанные в заявлении на отзыв регистрационного свидетельства SSL для юридического лица владелец доменного имени Интернет-ресурса, подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК ЦР представлением следующих документов:

1) заявление на отзыв SSL регистрационного свидетельства НУЦ РК (от юридического лица), полученное с Портала, содержащее уникальный номер и заверенное печатью юридического лица;

2) оригиналы документов, удостоверяющих личность представителя подписчика НУЦ РК (юридическое лицо владелец доменного имени интернет-ресурса).

3.4.9. Проверка (идентификация) подписчика НУЦ РК (участник информационной системы «Е-нотариат»)

Сведения, указанные в заявлении на отзыв регистрационного свидетельства для участника информационной системы «Е-Нотариат», подтверждаются при личном прибытии подписчика НУЦ РК либо представителя подписчика НУЦ РК ЦР представлением следующих документов:

1) заявление на отзыв регистрационного свидетельства, полученное с Портала и содержащее уникальный номер;

2) доверенность на представителя подписчика НУЦ РК (участника информационной системы «Е-нотариат») при представлении интересов заявителя третьим лицом в соответствии с п. 3.4.1 настоящей Политики;

3) оригиналы документов, удостоверяющих личность подписчика НУЦ РК (участника информационной системы «Е-нотариат»).

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

4.1. ПОРЯДОК ПОДАЧИ ЗАЯВЛЕНИЕ НА ВЫДАЧУ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ НУЦ РК

4.1.1. Лица, имеющие право подавать заявления на выдачу регистрационных свидетельств НУЦ РК

Заявление на выдачу регистрационного свидетельства НУЦ РК имеют право подавать:

физические лица;

юридические лица;

физические лица - нерезиденты;

юридические лица - нерезиденты.

участник информационной системы «Казначейство-Клиент».

4.1.2. Порядок регистрации и выдачи регистрационных свидетельств НУЦ РК

Регистрация заявителя в НУЦ РК, осуществляется в соответствии с пунктом 3.2. настоящих Правил.

4.1.3. Процедура генерации ключевой пары подписчика НУЦ РК

Заявители и подписчики НУЦ РК генерируют свои ключевые пары посредством Портала самостоятельно либо при личном обращении в ЦР в случае выпуска ЭЦП на удостоверении личности в соответствии с пунктом 6.1.2. настоящих Правил.

4.2. ОБРАБОТКА ЗАЯВЛЕНИЯ НА ВЫДАЧУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА НУЦ РК

4.2.1. Подтверждение принадлежности и действительности открытого ключа ЭЦП

Подтверждение принадлежности и действительности открытого ключа ЭЦП производится в соответствии с пунктом **Ошибка! Источник ссылки не найден.**настоящих Правил. При наличии действующего регистрационного свидетельства НУЦ РК подтверждение достоверности информации не проводится, и все действия по выдаче нового регистрационного свидетельства выполняются на Портале без необходимости личной явки в ЦР.

4.2.2. Отказ заявителю в приеме заявления на выдачу регистрационных свидетельств НУЦ РК

НУЦ РК отказывает заявителю:

в получении регистрационного свидетельства владельца в случае не представления необходимой информации и представления недостоверной информации

в отзыве регистрационного свидетельства владельца в случае ненадлежащего оформления соответствующего заявления на отзыв регистрационного свидетельства владельца и истечения срока действия регистрационного свидетельства владельца.

4.2.3. Срок рассмотрения заявлений на выдачу регистрационных свидетельств НУЦ РК

НУЦ РК рассматривает заявления на выдачу регистрационных свидетельств НУЦ РК заявителя в течение 2 рабочих дней.

4.3. ВЫДАЧА РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ПОДПИСЧИКОВ НУЦ РК

4.3.1. Действия НУЦ РК в ходе выдачи регистрационных свидетельств НУЦ РК

Регистрационные свидетельства НУЦ РК выдаются НУЦ РК заявителю на основании заявления, оформленного через Портал. Процедура выдачи регистрационного свидетельства НУЦ РК требует одной из форм подтверждения:

в случае отсутствия у подписчика действующего регистрационного свидетельства подписчика НУЦ РК — подтверждения принадлежности и действительности открытого ключа ЭЦП оператором ЦР;

при наличии действующего регистрационного свидетельства подписчика НУЦ РК — подписания заявления действующим ЭЦП и соответствующим регистрационным свидетельством подписчика НУЦ РК.

НУЦ РК генерирует ключевую пару и соответствующее регистрационное свидетельство подписчика НУЦ РК на основе информации, предоставленной в заявлении.

4.3.2. Уведомление подписчиков НУЦ РК о выдаче регистрационного свидетельства подписчика НУЦ РК

Официальным уведомлением о факте выдачи регистрационных свидетельств НУЦ РК является опубликование данных регистрационных свидетельств НУЦ РК в регистре регистрационных свидетельств НУЦ РК. При положительном результате обработки заявления на выдачу регистрационного свидетельства НУЦ РК, заявитель получает в качестве ответа выпущенные регистрационные свидетельства НУЦ РК.

НУЦ РК может направить извещение о выдаче регистрационных свидетельств подписчика НУЦ РК заявителю средствами электронной почты. В случае если подписчик НУЦ РК не получил данного уведомления, НУЦ РК ответственности не несёт.

4.4. ПРИНЯТИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА НУЦ РК ЗАЯВИТЕЛЕМ

4.4.1. Принятие регистрационного свидетельства НУЦ РК заявителем

Принятие заявителем регистрационных свидетельств НУЦ РК:

установка ключевой пары;

отсутствие возражений со стороны заявителя против принятия регистрационных свидетельств НУЦ РК или его содержания;

использование регистрационных свидетельств подписчиком НУЦ РК.

4.4.2. Уведомление НУЦ РК доверяющих сторон о выдаче регистрационных свидетельств подписчиков НУЦ РК

НУЦ РК направляет уведомление подписчику НУЦ РК посредством электронной почты на адрес, указанный при подаче заявления на выдачу регистрационных свидетельств НУЦ РК.

НУЦ РК не уведомляет доверяющие стороны о выпуске регистрационных свидетельств подписчиков НУЦ РК.

4.5. ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОЙ ПАРЫ И РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ПОДПИСЧИКА НУЦ РК

4.5.1. Использование закрытых ключей и регистрационных свидетельств подписчиками НУЦ РК

Подписчик НУЦ РК использует закрытый ключ после ознакомления и принятия им в полном объеме требований указанных в:

1) действующим законодательством Республики Казахстан;

2 Пользовательском соглашении;

3) политике применения регистрационных свидетельств НУЦ РК;

4) настоящих Правилах.

Подписчик НУЦ РК использует регистрационные свидетельства НУЦ РК в соответствии с политикой применения указанной в полях «keyUsage» и «extendedKeyUsage» согласно п.1.7.1-1.7.9. настоящих Правил.

Использование подписчиками регистрационных свидетельств НУЦ РК означает принятие положений настоящего Регламента и согласие на публикацию данных, не рассматриваемых в качестве конфиденциальных.

Подписчик НУЦ РК обязан принимать меры для защиты принадлежащего ему закрытого ключа ЭЦП от неправомерного доступа и использования, а также хранить открытые ключи в порядке, установленном действующим законодательством Республики Казахстан.

4.5.2. Использование открытых ключей и регистрационных свидетельств подписчиков НУЦ РК доверяющими сторонами

Участники ИОК, принимают обязательства регламентированные в:

действующем законодательстве Республики Казахстан;

Политике применения регистрационных свидетельств НУЦ РК;

настоящих Правилах;

Перед принятием решения о доверии к регистрационному свидетельству подписчика НУЦ РК, участники ИОК НУЦ РК должны выполнить следующие действия.

1) проверить соответствующий электронный документ, подписанный регистрационным(-и) свидетельством(-ами) подписчика НУЦ РК.

2) удостовериться в действительности регистрационного свидетельства подписчика НУЦ РК, выполнив следующие действия:

определить полную цепочку регистрационных свидетельств подписчиков НУЦ РК вплоть до корневого регистрационного свидетельства КУЦ РК;

оценить соответствие всех регистрационных свидетельств подписчиков НУЦ РК в цепочке следующим критериям:

сфера применения в соответствии Политикой применения регистрационных свидетельств подписчика НУЦ РК;

содержанию полей «keyUsage» и «extendedKeyUsage» регистрационного свидетельства согласно п.1.7.1-1.7.9. настоящих Правил;

удостовериться, что все регистрационные свидетельства подписчика НУЦ РК в цепочке подписаны КУЦ РК.

Информационные системы, относящиеся к участникам ИОК НУЦ РК, должны осуществлять соответствующую проверку согласно Правилам проверки электронной цифровой подписи и регистрационного свидетельства пользователей Национального удостоверяющего центра Республики Казахстан для информационных систем, доступных по адресу http://pki.gov.kz/images/content/doc/pravila.tiff.

4.6. ОБНОВЛЕНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

По запросу подписчика обновление данных подписчика НУЦ РК, внесение изменений и дополнений в структуру регистрационных свидетельств подписчика НУЦ РК и увеличение срока действия регистрационных свидетельств НУЦ РК, НУЦ РК не осуществляет.

В случае обновления персональных данных в регистрационных свидетельствах подписчика НУЦ РК, ему необходимо выпустить новое регистрационное свидетельство подписчика НУЦ РК в соответствии с пунктом **Ошибка! Источник ссылки не найден.** Правил и отозвать регистрационное свидетельство подписчика НУЦ РК в соответствии с пунктом 4.7 ниженастоящих Правил.

4.7. ОТЗЫВ РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ПОДПИСЧИКА НУЦ РК

4.7.1. Основания для отзыва регистрационных свидетельств подписчиков НУЦ РК

НУЦ РК отзывает регистрационные свидетельства подписчиков НУЦ РК до истечения срока действия в следующих случаях:

по требованию владельца регистрационного свидетельства либо его представителя;

смерти владельца регистрационного свидетельства;

предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;

по вступившему в законную силу решению суда;

на основании официального заявления на отзыв регистрационного свидетельства владельца по форме установленной действующим законодательством Республики Казахстан;

на основании вступившего в законную силу решения суда.

Отзыв регистрационного свидетельства владельца по требованию подписчика регистрационного свидетельства либо его представителя осуществляется в случаях:

использования регистрационного свидетельства владельца третьими лицами;

изменения фамилии, имени или отчества (при его наличии) подписчика регистрационного свидетельства;

смены наименования, реорганизации, ликвидации юридического лица;

в иных случаях.

4.7.2. Лица, имеющие право подавать заявления на отзыв регистрационных свидетельств подписчиков НУЦ РК

К лицам, имеющим право подавать заявления на отзыв регистрационных свидетельств подписчиков НУЦ РК относятся:

подписчики НУЦ РК;

представители подписчиков НУЦ РК.

4.7.3. Процедуры отзыва регистрационного свидетельства для всех участников ИОК НУЦ РК

Отзыв регистрационного свидетельства подписчика НУЦ РК осуществляется самим подписчиком посредством Портала, через «Личный кабинет». Также подписчик НУЦ РК может отозвать регистрационное свидетельство через ЦР.

После получения необходимых документов в течение 20 минут оператор ЦР осуществляет проверку (идентификацию) личности подписчика и проверку документов. В случае успешной проверки, оператор ЦР заполняет форму электронного заявления для отзыва регистрационного свидетельства и подтверждает электронный запрос путём удостоверения его своей ЭЦП, отправляет его в информационную систему и выдаёт подписчику или его представителю расписку о приёме документов.

4.7.4. Срок подачи заявлений на отзыв регистрационного свидетельства подписчика НУЦ РК

Подписчики НУЦ РК осуществляет своевременную подачу заявлений на отзыв регистрационных свидетельств НУЦ РК в порядке установленными настоящими Правилами.

4.7.5. Срок рассмотрения заявлений на отзыв регистрационного свидетельства подписчика НУЦ РК

НУЦ РК после получения заявления на отзыв регистрационного свидетельства осуществляет его рассмотрение и обработку в течение 2 рабочих дней. В случае успешного рассмотрения заявления, НУЦ РК осуществляет отзыв регистрационного свидетельства, публикует информацию об отозванном регистрационном свидетельстве в СОРС и уведомляет подписчика посредством электронной почты. НУЦ РК не несёт ответственности за получение подписчиком уведомления об отзыве регистрационного свидетельства.

4.7.6. Требования по проверке отзыва регистрационных свидетельств подписчика НУЦ РК для доверяющих сторон

Участники ИОК НУЦ РК должны проверять статус регистрационных свидетельств подписчиков НУЦ РК перед принятием решения об использовании указанных регистрационных свидетельств, посредством одного из следующих способов:

проверка наличия регистрационного свидетельства подписчика НУЦ РК в действующем СОРС;

проверка статуса регистрационного свидетельства подписчика НУЦ РК посредством службы OCSP.

НУЦ РК предоставляет необходимые механизмы проверки статуса регистрационных свидетельств в соответствии с настоящими Правилами.

4.7.7. Частота выпуска СОРС подписчиков НУЦ РК

СОРС подписчиков НУЦ РК выпускаются и публикуются раз в сутки. Также каждые два часа выпускается Дельта СОРС, содержащий перечень регистрационных свидетельств, отозванных с момента выпуска последнего СОРС.

4.7.8. Максимальная задержка СОРС подписчиков НУЦ РК

СОРС подписчиков НУЦ РК незамедлительно после генерации публикуются по адресам указанным в пунктом 2.2.1. настоящих Правил.

4.7.9. Требование по доступности СОРС и информации о статусе регистрационных свидетельств подписчика НУЦ РК

НУЦ РК обеспечивает непрерывную доступность службы СОРС и информации о статусе регистрационных свидетельств подписчика НУЦ РК в соответствии с настоящими Правилами.

4.7.10. Требования проверки отзыва онлайн

В соответствии с положениями пункта 4.7.6. настоящих Правил.

4.8. СЛУЖБЫ ПРОВЕРКИ СТАТУСА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКОВ НУЦ РК

4.8.1. Эксплуатационные характеристики

Информация о статусе регистрационных свидетельств подписчиков НУЦ РК доступна по адресам указанным в пунктом 2.2.1. настоящих Правил через службы СОРС и OCSP.

4.8.2. Режим работы служб НУЦ РК

Службы проверки статуса регистрационных свидетельств НУЦ РК доступны 24 часа в сутки, 7 дней в неделю.

4.9. ОКОНЧАНИЕ СРОКА ДЕЙСТВИЯ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

Регистрационное свидетельство подписчика НУЦ РК становится недействительным при истечении срока действия в соответствии с пунктом 6.3.2 ниже настоящих Правил.

Подписчик НУЦ РК вправе отозвать регистрационное свидетельство подписчика НУЦ РК до окончания срока его действия в соответствии с пунктом 4.7 вышенастоящих Правил.

4.10. ДЕПОНИРОВАНИЕ И ВОССТАНОВЛЕНИЕ КЛЮЧЕВОЙ ПАРЫ

НУЦ РК не допускает депонирование и восстановление ключевых пар подписчиков и НУЦ РК.

5. УПРАВЛЕНЧЕСКИЕ, ОПЕРАЦИОННЫЕ И ФИЗИЧЕСКИЕ КОНТРОЛИ АКТИВОВ НУЦ РК

5.1. КОНТРОЛЬ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ АКТИВОВ НУЦ РК

НУЦ РК обеспечивает физическую безопасность активов НУЦ РК в соответствии с действующим законодательством Республики Казахстан. Детальные политики и процедуры мер обеспечения физической безопасности содержат конфиденциальную информацию НУЦ РК и поэтому не публикуются. НУЦ РК обеспечивает физическую безопасность активов НУЦ РК посредством организационно-технических и административных мероприятий, направленных на:

обеспечение физической безопасности работников НУЦ РК;

обеспечение правильности функционирования аппаратного обеспечения систем НУЦ РК, а также систем передачи и хранения информации НУЦ РК и носителей информации, относящейся к НУЦ РК;

обеспечения информационной безопасности НУЦ РК;

контроль эффективности физической безопасности НУЦ РК.

5.1.1. Место размещения активов НУЦ РК

В зданиях, в которых находятся места размещения активов НУЦ РК, обеспечиваются следующие условия:
обеспечение физической безопасности деятельности НУЦ РК в соответствии с пунктом 5.1 вышенастоящих Правил;
обеспечение резервных объектов для поддержания непрерывности деятельности НУЦ РК в случаях чрезвычайной ситуации.

5.1.2. Физический доступ к информационным активам НУЦ РК

Информационные активы НУЦ РК защищены минимум четырьмя последовательными уровнями физической безопасности, характеризующимися последовательно усиливающимися требованиями по физическому доступу на каждый следующий уровень в соответствии с:
внутренними политиками НУЦ РК по организации физической безопасности и разделения полномочий;
внутренними политиками организаций, обеспечивающих размещение систем НУЦ РК;
законодательством Республики Казахстан.
Функционирование уровней безопасности обеспечивается техническими и организационными мерами, направленными на:
предотвращение несанкционированного физического доступа — посредством систем ограничения физического доступа (турникеты, запирающиеся двери, охрана, дежурные);
автоматическую фиксацию случаев физического доступа — посредством видеонаблюдения и записи случаев физического доступа для двух уровней максимального ограничения физического доступа (автоматическим и ручным ведением журналов);
реагирование уполномоченными подразделениями на несанкционированные попытки получения физического доступа — посредством охраны, сигнализации и систем видеонаблюдения;
безопасность хранения носителей данных с ключевым материалом НУЦ РК — посредством использования сейфов и безопасных устойчивых к взлому контейнеров в физически безопасных местах, с обязательным протоколированием случаев доступа к сейфам и контейнерам, в которых хранился ключевой материал НУЦ РК, а также посредством организационных мероприятий, гарантирующих работу с носителями данных исключительно в присутствии ответственных уполномоченных работников НУЦ РК.

5.1.3. Электропитание и поддержание микроклимата в местах размещения аппаратного обеспечения НУЦ РК

Места размещения аппаратного обеспечения НУЦ РК, поддерживающего работу информационных активов НУЦ РК, оборудованы с учётом следующих критериев:
обеспечивается непрерывность электроснабжения при помощи систем основного, резервного и аварийного электроснабжения;
обеспечивается микроклимат, необходимый для функционирования аппаратного обеспечения систем НУЦ РК при помощи основных и запасных систем контроля температуры, влажности и вентиляции в соответствии с действующими стандартами Республики Казахстан, а также технической и эксплуатационной документацией аппаратного обеспечения.

5.1.4. Влияние природных стихий на места размещения аппаратного обеспечения

Места размещения аппаратного обеспечения систем НУЦ РК определены с учётом минимизации рисков природных стихий, таких как землетрясения, наводнения, оползни, сели, ураганы и т.д.

5.1.5. Предотвращение и защита от пожаров мест размещения аппаратного обеспечения

Места размещения аппаратного обеспечения информационных активов НУЦ РК обеспечивают эффективное предупреждение и борьбу с пожарами, вредными воздействиями возгорания и задымления в соответствии с действующим законодательством Республики Казахстан.

5.1.6. Хранение носителей информации НУЦ РК

Все носители информации НУЦ РК, включая исходные коды, данные, автоматические журналы, резервные копии хранятся с обеспечением физической безопасности в соответствии с:
внутренними политиками НУЦ РК по организации физической и информационной безопасности, а также разделения полномочий;
внутренними политиками организаций, обеспечивающих размещение носителей информации НУЦ РК;
действующим законодательством Республики Казахстан.
НУЦ РК обеспечивает защиту носителей информации НУЦ РК от:
нарушения вышеперечисленных регламентов;
повреждения;
неавторизованного изменения информации;
раскрытия конфиденциальной информации.

5.1.7. Утилизация носителей информации НУЦ РК и аппаратного обеспечения

НУЦ РК обеспечивает утилизацию носителей информации НУЦ РК и аппаратного обеспечения в соответствии с:
внутренними политиками НУЦ РК по организации физической и информационной безопасности, а также разделения полномочий;
внутренними политиками организаций, обеспечивающих размещение носителей информации и систем НУЦ РК;
действующим законодательством Республики Казахстан;
технической документацией для носителей информации НУЦ РК и аппаратного обеспечения.
Все носители, на которых когда-либо хранилась конфиденциальная информация, приводятся в состояние непригодности для чтения. НУЦ РК обеспечивает утилизацию носителей информации криптографического аппаратного обеспечения в соответствии с пунктом 6.2.1 ниженастоящих Правил).

5.1.8. Резервное копирование информации НУЦ РК

НУЦ РК осуществляет резервное копирование программного обеспечения систем НУЦ РК, их данных, журналов, конфиденциальной информации и СОРС.

Носители резервных копий хранятся с обеспечением физической безопасности для предотвращения:

несанкционированного доступа к резервным копиям;

искажения резервных копий;

уничтожения резервных копий.

5.2. ОТВЕТСВЕННОСТЬ И КОНТРОЛЬ В ДЕЯТЕЛЬНОСТИ НУЦ РК

5.2.1. Распределение ответственных ролей

К разряду ответственного персонала относятся работники РГП ГТС, имеющие доступ или контролирующие аутентификацию и операции, которые могут существенно влиять на следующие функции НУЦ РК:

проверка информации из заявлений на выдачу регистрационных свидетельств;

приём, отказ в приёме или иную обработку заявлений на выдачу или отзыв регистрационных свидетельств;

выдача или отзыв регистрационных свидетельств.

Ответственные роли включают, но не ограничиваются следующими функциями:

обслуживание подписчиков НУЦ РК;

операции с криптографическим аппаратным обеспечением;

управление и обеспечение информационной безопасности;

управления и обеспечение физической безопасности;

администрирование программного обеспечения систем НУЦ РК;

обслуживание аппаратного обеспечения систем НУЦ РК;

управление и обеспечение обслуживающей инфраструктуры НУЦ РК.

НУЦ РК обеспечивает соответствие работников всех ответственных ролей квалификационным требованиям в соответствии с пунктами 5.2.3 ниже3.1. и 5.3.2 ниженастоящих Правил.

5.2.2. Численность персонала, необходимого для отдельной задачи

РГП ГТС обеспечивает необходимое количество подразделений и работников для функционирования системы внутренних контролей. В случае вакантности штатной единицы, необходимой для осуществления контроля, РГП ГТС принимает альтернативные меры контроля исходя из оценки рисков.

В частности, задачи по управлению жизненным циклом регистрационных свидетельств подписчиков НУЦ РК предполагают участие как минимум двух независимых сторон — оператора ЦР и ответственного работника РГП ГТС. Также задачи по управлению ключевым материалом НУЦ РК, управлению доступом к информационной системе НУЦ РК, управлению изменениями в системах НУЦ РК, резервным копированием систем НУЦ РК и т.д. предполагают участие не менее двух работников, относящихся к двум независимым подразделениям РГП «ГТС».

5.2.3. Идентификация и аутентификация ответственной роли

Для каждой роли НУЦ РК определены должностные инструкции и квалификационные требования. Для каждого из работников РГП ГТС перед приёмом на работу проверяется соответствие квалификационным требованиям в соответствии с пунктом 5.3.2 ниженастоящих Правил, а также проводится подтверждение личности кандидата и сбор прочих документов в соответствии с законодательством Республики Казахстан.

Служебная деятельность работников РГП ГТС в ответственных ролях возможна только в пределах физически защищённого периметра здания РГП ГТС в соответствии с пунктом 5.1.2 вышенастоящих Правил. Доступ работников в защищённый периметр сопровождается подтверждением личности работников. Работа с информационными системами НУЦ РК также сопровождается подтверждением личности работников.

5.2.4. Функции ИОК НУЦ РК, требующие разделения обязанностей

НУЦ РК различает несовместимые функции, требующие разделения обязанностей. К таким относятся:

администрирование информационных систем НУЦ РК;

разработка систем НУЦ РК;

работа операторов ЦР.

НУЦ РК обеспечивает соблюдение разделения несовместимых функций во всех своих процессах.

5.3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РАБОТНИКОВ НУЦ РК

РГП ГТС и РГП ЦОН обеспечивают безопасность работников РГП ГТС в соответствии с:

внутренними политиками НУЦ РК по организации физической безопасности;

внутренними политиками организаций, обеспечивающих размещение систем и работников НУЦ РК;

законодательством Республики Казахстан.

Детальные меры по обеспечению физической безопасности работников РГП ГТС формализованы и утверждены документально, однако не публикуются, поскольку содержат конфиденциальную информацию НУЦ РК.

5.3.1. Требования к опыту и квалификации работников РГП ГТС и операторов ЦР

РГП ГТС и РГП ЦОН обеспечивают соответствие работников минимальным требованиям к опыту и квалификации в соответствии с:

внутренними кадровыми политиками и должностными инструкциями РГП ГТС или РГП «ЦОН»;

внутренними политиками организаций, обеспечивающих работу информационной системы НУЦ РК;

законодательством Республики Казахстан.

Подтверждение соответствия требованиям к опыту и квалификации осуществляется предоставлением подтверждающих дипломов, сертификатов, рекомендаций и т.д., с сохранением копий в соответствующих отделах кадров.

5.3.2. Процедуры проверки работников РГП ГТС и операторов ЦР

РГП ГТС и РГП «ЦОН» обеспечивают проверку работников перед приёмом и в течение действия трудового договора в соответствии с:

внутренними кадровыми политиками и должностными инструкциями РГП ГТС или РГП «ЦОН»;

внутренними политиками организаций, обеспечивающих работу информационных систем НУЦ РК;

действующим законодательством Республики Казахстан.

Проверки включают, как минимум, документальное подтверждение следующих вопросов:

соответствие требованиям к опыту и квалификации в соответствии с пунктом 5.3.1 вышенастоящих Правил;

предоставление необходимых справок и подтверждений в соответствии с действующим законодательством Республики Казахстан и ролью оператора ЦР или работника РГП ГТС.

5.3.3. Требования к повышению квалификации работников РГП ГТС

РГП ГТС обеспечивает повышению квалификации работников с целью компетентного и качественного выполнения служебных обязанностей. Повышение квалификации работников РГП ГТС осуществляется посредством подготовки, переподготовки и повышения квалификации в соответствии с должностными обязанностями. Мероприятия по повышению квалификации работников включают прохождение необходимых курсов и посещения обучающих мероприятий.

5.3.4. Периодичность повышения квалификации работников РГП ГТС

Периодичность мероприятий по повышению квалификации работников РГП ГТС определяется в соответствии с:

потребностями в целях осуществления деятельности НУЦ РК;

внутренними кадровыми политиками и должностными инструкциями;

законодательством Республики Казахстан.

5.3.5. Перемещения работников РГП ГТС по службе

Перемещения работников НУЦ РК по службе определяется в соответствии с:

потребностями в целях осуществления деятельности НУЦ РК;

внутренними кадровыми политиками, должностными инструкциями и планами НУЦ РК и РГП «ГТС»;

законодательством Республики Казахстан.

Решения по перемещениям работников РГП ГТС утверждаются директором РГП «ГТС» или уполномоченным заместителем.

5.3.6. Ответственность работника РГП ГТС за несанкционированные действия

Работники РГП «ГТС», а также операторы ЦР несут ответственность за соблюдение внутреннего распорядка в соответствии с:

внутренними политиками и должностными инструкциями работников РГП ГТС и РГП «ГТС» или РГП «ЦОН»;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

законодательством Республики Казахстан.

При обнаружении несанкционированных действий или подозрении на совершение несанкционированных действий, лицо, обнаружившее нарушение, сообщает об этом департаменту информационной безопасности НУЦ РК. Ответственный работник департамента информационной безопасности РГП ГТС принимает решение о необходимости срочного блокирования доступа нарушителя (подозреваемого) к системам и регистрирует инцидент. Дальнейшие мероприятия по расследованию инцидента, а также определение мер ответственности осуществляются в порядке, определённом вышеуказанными регламентами.

5.3.7. Требования к независимым сторонам

НУЦ РК не допускает независимые стороны, не относящиеся к НУЦ РК, к непосредственной работе с информационными системами, обеспечивающими деятельность НУЦ РК. Независимые стороны могут присутствовать при некоторых процедурах НУЦ РК в качестве участников или наблюдателей.

К участию в качестве независимых наблюдателей допускаются:

уполномоченные органы, имеющие отношение к функционированию ИОК НУЦ РК или ИОК КУЦ РК (например, КНБ РК, Канцелярия Премьер-министра Республики Казахстан, владельцы систем «Е-Нотариат», «Казначейство-Клиент», портала «электронного правительства» и т.д.); а также

сертифицирующие органы на основании договоров о выполнении услуг и соглашений о неразглашении (например, для целей сертификации оборудования НУЦ РК, аудиторы WebTrust и т.д.).

5.3.8. Документация, раскрываемая работникам РГП ГТС, а также оператором ЦР

РГП ГТС обеспечивает работников, а также операторов ЦР минимумом необходимых материалов в целях:

обучения и повышению квалификации в соответствии с должностными инструкциями в соответствии с пунктом 5.3.3 вышенастоящих Правил;

выполнения должностных обязанностей.

Обеспечение материалами осуществляется в соответствии с:

внутренними политиками и должностными инструкциями РГП ГТС;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

законодательством Республики Казахстан.

5.4. ДОКУМЕНТИРОВАНИЯ СОБЫТИЙ (ЖУРНАЛИРОВАНИЕ) В ИНФОРМАЦИОННОЙ СИСТЕМЕ НУЦ РК

5.4.1. Типы журналируемых событий

НУЦ РК осуществляет ведение и хранение журналов для следующих типов событий:

1) События управления жизненным циклом ключевых пар НУЦ, в том числе:

генерация, резервное копирование, хранение, восстановление, архивирование и уничтожение закрытых ключей НУЦ РК;

события управления жизненным циклом аппаратного обеспечения, поддерживающего работу ключевых пар НУЦ РК.

2) События управления жизненным циклом регистрационных свидетельств НУЦ РК, в том числе:

подача заявления на выдачу и отзыв регистрационного свидетельства НУЦ РК;

успешная или неудавшаяся обработка запросов на выдачу и отзыв регистрационных свидетельств НУЦ РК;

генерация и публикация СОРС.

3) События, связанные с обеспечением физической и информационной безопасности НУЦ РК:

обновление или модификация систем НУЦ РК, настроек систем НУЦ РК или систем, поддерживающих работу НУЦ РК;

управление доступом к системам НУЦ РК или смена политик управления доступом (в том числе, роли и профили пользователей);

события информационной безопасности (в том числе попытки получения доступа к конфиденциальной информации и системам НУЦ РК — как успешные, так и неудавшиеся);

программные и аппаратные сбои и ошибки информационных систем НУЦ РК;

события физического доступа в соответствии с политикой физического доступа;

данные о функционировании систем поддержания электроснабжения и микроклимата.

Структура записи журналов определяется технической документацией, но включает в себя как минимум следующие элементы:

дата и время записи;

порядковый номер записи;

тип события;

источник записи.

В случае невозможности записи в журнале какого-либо из перечисленных выше элементов, НУЦ РК прибегает к альтернативным техническим и организационным мерам в целях минимизации рисков.

НУЦ РК не допускает записи в явном виде ключей и паролей.

5.4.2. Частота анализа контрольных протоколов

НУЦ РК осуществляет ежедневный анализ журналов в целях функционирования системы внутренних контролей НУЦ РК.

5.4.3. Срок хранения журналов

НУЦ РК хранит журналы в течение 30 календарных дней, после чего журналы подлежат архивированию и сдаче в архив в соответствии с пунктом 5.5 ниже Правил.

5.4.4. Защита журналов

НУЦ РК обеспечивает защиту журналов от несанкционированного просмотра, модификации и удаления. Защита журналов обеспечивается организационными и техническими мерами, в том числе посредством подписания всех журналов выделенным регистрационным свидетельством НУЦ РК.

5.4.5. Резервное копирование журналов

НУЦ РК осуществляет резервное копирование журналов на ежедневной основе. Резервные копии хранятся в соответствии с:

внутренними политиками РГП «ГТС» по физической и информационной безопасности;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

требованиями законодательства Республики Казахстан.

5.4.6. Система сбора журналов

Не используется.

5.4.7. Уведомление субъекта, вызвавшего событие

Не оговаривается.

5.4.8. Оценка уязвимостей НУЦ РК

НУЦ РК осуществляет периодическую оценку уязвимостей, а также уязвимостей, выявленных в рамках работы системы

внутренних контролей НУЦ РК в соответствии с:

внутренними политиками РГП «ГТС» (в том числе в соответствии с регламентом порядка проведения периодических оценок уязвимостей, управления рисками и управления инцидентами);

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

требованиями законодательства Республики Казахстан.

5.5. АРХИВ ЗАПИСЕЙ

5.5.1. Типы архивируемых событий

НУЦ РК обеспечивает архивное хранение следующих типов информации в соответствии с требованиями действующего законодательства Республики Казахстан:

журналы событий;

действующие, отозванные и истёкшие регистрационные свидетельства подписчиков;

действующие, отозванные и истёкшие регистрационные свидетельства НУЦ РК;

заявления на выдачу и отзыв регистрационных свидетельств подписчиков;

списки отозванных регистрационных свидетельств подписчиков и НУЦ РК.

5.5.2. Срок хранения архива

НУЦ РК обеспечивает непрерывную работу архива в соответствии с требованиями действующего законодательства Республики Казахстан. Длительность архивного хранения данных устанавливается в соответствии с:

внутренними политиками РГП «ГТС» для каждого вида данных;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

действующим законодательством Республики Казахстан.

5.5.3. Защита архива

НУЦ РК обеспечивает защиту архивных материалов в соответствии:

внутренними политиками РГП «ГТС» для каждого вида данных;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

действующим законодательством Республики Казахстан.

Доступ в архив ограничен только ответственными работниками РГП ГТС. НУЦ РК использует технические и организационные меры по защите архивным материалов от несанкционированного доступа, модификации или уничтожения.

5.5.4. Резервное копирование архива

Данные, хранящиеся в архиве, резервируются на ежемесячной основе. Резервные копии архива хранятся в физически защищённом месте хранения в соответствии с требованиями действующего законодательства Республики Казахстан.

5.5.5. Требование о постановке отметки времени на архивных записях

НУЦ РК ведёт автоматический реестр архивных материалов с автоматизированным указанием даты занесения в архив. Реестр архивных материалов подписывается корневым сертификатом НУЦ РК.

5.5.6. Условия архивирования

Архивирование материалов осуществляется в соответствии с:

внутренними политиками РГП «ГТС» для каждого вида данных;

внутренними политиками организаций, обеспечивающих работу систем НУЦ РК;

законодательством Республики Казахстан.

5.5.7. Порядок получения и проверки архивной информации

Доступ к архивным материалам ограничен в соответствии с пунктом 5.5.3 настоящих Правил выше. Ответственные работники РГП ГТС осуществляют проверку архивной информации в соответствии с положениями пунктом 5.7.4 ниженастоящих Правил.

5.6. ЗАМЕНА КЛЮЧЕЙ НУЦ РК

НУЦ РК осуществляет замену ключевых пар ключевых пар и регистрационных свидетельств НУЦ РК по истечении срока действия корневого регистрационного свидетельства или в случае компрометации ключевых пар. При этом НУЦ РК:

прекращает использование старых ключевых пар и соответствующих им регистрационных свидетельств;

генерирует новые ключевые пары и соответствующие корневые регистрационные свидетельства.

Генерация ключевых пар НУЦ РК осуществляется в присутствии независимой стороны в качестве наблюдателя.

5.7. КОМПРОМЕТАЦИЯ И АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ КЛЮЧЕЙ НУЦ РК

5.7.1. Процедуры обработки происшествий и компрометации

НУЦ РК обеспечивает создание и безопасное хранение резервных копий критических данных на случай чрезвычайных происшествий или компрометации;

заявления на выдачу и изменение статуса регистрационных свидетельств;
журналы событий;
списки отозванных регистрационных свидетельств;
ключевые пары НУЦ РК.

По фактами происшествий в НУЦ РК, а также при обнаружении факта компрометации или подозрению на компрометацию закрытых ключей НУЦ РК проводятся процедуры в соответствии с требованиями законодательства Республики Казахстан и внутренними регламентами НУЦ РК с целью:

оценки и категоризации события;
принятия мер по предупреждению или ликвидации последствий события в соответствии с оценкой рисков НУЦ РК.

5.7.2. Повреждения вычислительных, программных ресурсов и/или данных

Повреждения вычислительных, программных ресурсов и/или данных НУЦ РК рассматриваются как происшествия и обрабатываются в соответствии с положениями пунктом 5.7.1 вышенастоящих Правил.

5.7.3. Компрометация закрытого ключа НУЦ РК

НУЦ РК обеспечивает работу системы внутренних контролей, включающую мониторинг на предмет возможной компрометации закрытых ключей НУЦ РК. В случае обнаружения компрометации или наличия обоснованных подозрений в компрометации закрытых ключей НУЦ РК вступает в действие План восстановления деятельности в соответствии с положениями пунктом 5.7.4 ниже.

В случае если необходимо перевыпустить ключевые пары НУЦ РК, выполняется процедура в соответствии с пунктом 6.1 ниже. При этом обеспечивается уведомление всех участников ИОК НУЦ РК о факте перевыпуска ключевых пар НУЦ РК.

5.7.4. Возможности непрерывной деятельности после происшествий

В НУЦ РК принят утверждённый и протестированный детальный План восстановления деятельности, нацеленный на смягчение последствий реализации угроз, в том числе катастроф природного характера. План восстановления деятельности регулярно рассматривается на предмет необходимости обновления в соответствии с внутренними процедурами оценки рисков НУЦ РК.

НУЦ РК обладает резервными объектами с целью обеспечения непрерывности служб и ключевых функций НУЦ РК. Информация основного объекта НУЦ РК синхронизируется с резервными объектами в режиме онлайн.

НУЦ РК обеспечивает восстановление основных объектов, служб и функций в течение не более 24 часов после реализации угрозы непрерывности деятельности; в течение этого времени службы и функции НУЦ РК поддерживаются резервными объектами. Полное восстановление обеспечивается в срок не более 7 календарных дней. При этом восстановление на основном объекте таких функций как выдача и отзыв регистрационных свидетельств подписчиков, а также публикация сведений об отзыве регистрационных свидетельств подписчиков осуществляется в течение не более чем 2 часов.

В целях тестирования возможностей непрерывной деятельности, НУЦ РК производит регулярное переключение обработки с основного объекта на резервный.

5.8. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ НУЦ РК ИЛИ ЦР

В случае необходимости прекращения деятельности НУЦ РК или ЦР, НУЦ РК предпринимает все меры, необходимые для заблаговременного уведомления об этом подписчиков и участников ИОК НУЦ РК. Далее НУЦ РК разрабатывает план прекращения деятельности с целью минимизации неудобств для подписчиков и участников ИОК НУЦ РК. План прекращения может включать в себя следующие вопросы:

уведомление с информацией о статусе НУЦ РК для сторон, которых касается прекращение, в том числе подписчиков и участников ИОК НУЦ РК;

сохранение архивов НУЦ РК в соответствии с требованиями законодательства Республики Казахстан и соответствующей Политикой применения регистрационных свидетельств;

продолжение сервисов поддержки подписчиков и клиентов;
продолжение сервисов проверки отзыва, таких как служба OCSP и выпуск списков отозванных регистрационных свидетельств;
отзыв действующих не отозванных регистрационных свидетельств подписчиков, при необходимости;
выпуск заменяющих регистрационных свидетельств удостоверяющим центром-правопреемником;
дальнейшее местонахождение закрытых ключей НУЦ РК и криптографических модулей, содержащих эти закрытые ключи;
положения, необходимые для передачи сервисов НУЦ РК его правопреемнику.

6. КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ НУЦ РК

6.1. ВЫПУСК И УСТАНОВКА КЛЮЧЕВЫХ ПАР НУЦ РК И ПОДПИСЧИКОВ НУЦ РК

6.1.1. Генерация ключевой пары

НУЦ РК генерирует все ключевые пары, использующиеся в ИОК НУЦ РК. Генерация ключевых пар осуществляется при помощи криптографических модулей, сертифицированных на соответствие действующему стандарту Республики Казахстан СТ РК 1073-2007 по уровню не ниже второго.

Генерация ключевых пар самого НУЦ РК осуществляется исключительно в соответствии с утверждённым внутренним регламентом, при участии компетентных ответственных работников и при наблюдении независимой стороны. Церемония генерации ключевых пар НУЦ РК актируется соответствующим протоколом за подписью всех участников церемонии. Протоколы хранятся и

архивируются в соответствии с требованиями действующего законодательства Республики Казахстан и внутренними регламентами НУЦ РК.

6.1.2. Доставка закрытого ключа подписчику НУЦ РК

В настоящее время НУЦ РК выпускает ключевые пары подписчиков НУЦ РК только на следующих видах носителей:

1) на удостоверении личности (для физических лиц, граждан Республики Казахстан);

2) непосредственно на сертифицированном защищённом носителе, исключающем возможность компрометации ключевого материала (разглашения или модификации) — таких, как KazToken, JaCarta и т.д.; или

3) на файловой системе подписчика.

Ключевые пары подписчиков НУЦ РК защищаются при помощи пароля (см. пунктом 6.2.8 ниже).

Запись ключевых пар на удостоверении личности осуществляется одним из следующих способов:

1) в случае самостоятельной подачи заявления на выдачу регистрационного свидетельства онлайн — самостоятельно заявителем при помощи кардридера; или

2) при личном обращении заявителя или его представителя в ЦР — оператором ЦР при помощи кардридера в ЦР.

Запись ключевых пар на защищённый носитель осуществляется одним из следующих способов:

1) в случае самостоятельной подачи заявления на выдачу регистрационного свидетельства онлайн — самостоятельно заявителем на сертифицированный защищённый носитель; или

2) при личном обращении заявителя или его представителя в ЦР — оператором ЦР на защищённый носитель KazToken.

НУЦ РК поддерживает внутренние контроли посредством организационных и технических мер для исключения хранения закрытых ключей подписчиков в НУЦ РК в каком-либо виде.

6.1.3. Доставка открытого ключа подписчика НУЦ РК в НУЦ РК

Открытый ключ подписчика НУЦ РК генерируется в составе ключевой пары на Портале НУЦ РК и, таким образом, не требует доставки в НУЦ РК.

6.1.4. Передача открытого ключа КУЦ РК доверяющим сторонам

Открытый ключ КУЦ РК доступен в составе корневого регистрационного свидетельства КУЦ РК на интернет-ресурсе НУЦ РК обеспечивает организационно-технические меры по обеспечению целостности и достоверности открытого ключа НУЦ РК.

6.1.5. Размеры ключевой пары

Ключевые пары подписчиков НУЦ РК выпускаются в соответствии с алгоритмом RSA (PKCS#1) и имеют длину:
закрытый ключ — 2048 бит;
открытый ключ — 2048 бит.
Также НУЦ РК выпускает ключевые пары подписчиков юридических лиц в соответствии с алгоритмом ГОСТ и имеющие длину:
закрытый ключ — 256 бит;
открытый ключ — 512 бит.

6.1.6. Цели использования ключевой пары

В соответствии с пунктом **Ошибка! Источник ссылки не найден.**настоящих Правил.

6.2. КОНТРОЛИ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ НУЦ РК И ПОДПИСЧИКОВ НУЦ РК, А ТАКЖЕ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ КРИПТОГРАФИЧЕСКОГО АППАРАТНОГО ОБЕСПЕЧЕНИЯ НУЦ РК

НУЦ РК поддерживает внутреннюю контрольную среду с целью защиты закрытых ключей НУЦ РК и безопасного управления жизненным циклом криптографического аппаратного обеспечения НУЦ РК.

6.2.1. Стандарты и контроль криптографического аппаратного обеспечения

Криптографическое аппаратное обеспечение НУЦ РК сертифицировано на соответствие действующему в Республике Казахстан стандарту СТ РК 1073-2007, определяющему общие технические требования к средствам криптографической защиты информации на соответствие не ниже, чем второму уровню безопасности.

НУЦ РК реализует ряд технических и организационных мер в целях обеспечения конфиденциальности и целостности криптографического аппаратного обеспечения при транспортировке, пуско-наладочных работах и эксплуатации в основных и резервных объектах НУЦ РК. НУЦ РК также реализует ряд технических и организационных мер для обеспечения эксплуатации и обслуживания криптографического аппаратного обеспечения в строгом соответствии с его технической и эксплуатационной документацией, а также внутренними правилами физической безопасности в соответствии с пунктом 5.1 вышенастоящих Правил и процедурными правилами с. пунктом 5.2 вышенастоящих Правил.

Криптографическое аппаратное обеспечение НУЦ РК хранится и эксплуатируется только в предназначенных для этого защищённых объектах НУЦ РК. Вывод криптографического аппаратного обеспечения НУЦ РК из использования для ремонтных работ сопровождается гарантированной очисткой и, при возможности, физическим уничтожением накопителей памяти устройства. Окончательный вывод криптографического аппаратного обеспечения НУЦ РК из использования сопровождается физическим уничтожением криптографического аппаратного обеспечения в защищённой среде.

Мероприятия по приёму, обслуживанию и выводу из эксплуатации криптографического аппаратного обеспечения НУЦ РК осуществляются в присутствии ответственных работников, включенных в список доверенных ролей в соответствии с. пунктом 5.2

вышенастоящих Правил.

6.2.2. Разделение закрытого ключа НУЦ РК между ответственными сторонами по схеме m из n

Криптографические операции, проводимые вручную и требующие использования закрытых ключей НУЦ РК, осуществляются с использованием резервной копии закрытого ключа НУЦ РК, защищённого при помощи разделённого секрета. Для этого информация, необходимая для восстановления резервной копии закрытого ключа НУЦ РК («секрет») делятся на n частей. Для успешного восстановления резервной копии закрытого ключа НУЦ РК требуется не менее m частей секрета. При генерации секрета значения m и n определяются по формуле: $n > m + 1$.

Части секрета хранятся ответственными участниками церемонии генерации ключевых пар НУЦ РК в соответствии с требованиями законодательства Казахстан и внутренней регламентной документацией НУЦ РК в соответствии с пунктом 6.4.1 ниже.

6.2.3. Депонирование закрытых ключей подписчиков НУЦ РК

Закрытые ключи подписчиков НУЦ РК не депонируются.

6.2.4. Резервное копирование закрытого ключа НУЦ РК

На случай повреждения или недоступности закрытых ключей НУЦ РК, при генерации ключевых пар НУЦ РК создаются их резервные копии. Резервная копия закрытого ключа НУЦ РК защищается секретом в соответствии с положениями пунктом 6.2.2 выше.

6.2.5. Архивирование закрытого ключа НУЦ РК

Архивирование закрытых ключей НУЦ РК с истекшим сроком действия не допускается.

6.2.6. Импорт и экспорт закрытых ключей НУЦ РК, хранящихся в криптографических модулях

Ключевой материал НУЦ РК вне криптографических модулей существует исключительно в зашифрованном виде с обеспечением целостности и конфиденциальности ключевого материала НУЦ РК.

Экспорт ключевого материала из криптографических модулей НУЦ РК возможен только в виде резервной копии закрытого ключа в соответствии с пунктом 6.2.4 выше.

6.2.7. Хранение закрытого ключа НУЦ РК в криптографическом модуле и закрытых ключей подписчиков в защищённых носителях

Криптографические модули, хранящие закрытые ключи НУЦ РК, аппаратно не допускают хранения ключевого материала в незашифрованном виде, в том числе в оперативной памяти устройства.

Закрытые ключи подписчиков НУЦ РК, хранящиеся в сертифицированных защищённых носителях, хранятся в соответствии с требованиями стандарта PKCS#11.

6.2.8. Способы активации закрытого ключа НУЦ РК и подписчиков

Закрытые ключи НУЦ РК перед использованием вручную активируются в соответствии с положениями, описанными в пунктом 6.2.2 выше.

Закрытые ключи подписчиков НУЦ РК перед использованием активируются при задании пароля. Дальнейшее использование закрытых ключей возможно только с вводом пароля.

6.2.9. Способ уничтожения закрытого ключа НУЦ РК и подписчиков НУЦ РК

Все части закрытых ключей НУЦ РК, выведенные из эксплуатации, уничтожаются с гарантированной невозможностью восстановления. Процедура уничтожения закрытого ключа НУЦ РК осуществляется уполномоченными работниками в присутствии независимого наблюдателя.

Уничтожение закрытых ключей подписчиков НУЦ РК является ответственностью подписчиков НУЦ РК.

6.2.10.Оценка криптографических модулей НУЦ РК

Все криптографические модули, используемые НУЦ РК, сертифицированы на соответствие требованиям применимого действующего стандарта Республики Казахстан СТ РК 1073-2007 не ниже чем по второму уровню. Использование несертифицированных криптографических модулей не допускается в соответствии с внутренними регламентами НУЦ РК, настоящими Правилами и Политикой применения регистрационных свидетельств.

6.3. ДРУГИЕ АСПЕКТЫ УПРАВЛЕНИЯ КЛЮЧЕВОЙ ПАРОЙ НУЦ РК

6.3.1. Архивирование открытых ключей

Все открытые ключи НУЦ РК и подписчиков НУЦ РК, для которых НУЦ РК когда-либо выдавал регистрационные свидетельства, архивируются в составе соответствующих регистрационных свидетельств в соответствии с положениями пунктом 5.5 выше.

6.3.2. Сроки действия регистрационных свидетельств НУЦ РК и использования ключевых пар

Регистрационные свидетельства НУЦ РК выдаются со сроком действия в 5 лет. Регистрационные свидетельства подписчиков НУЦ РК выпускаются со сроком действия в 1 год. Регистрационные свидетельства служб TSP и OSCP НУЦ РК выпускаются со сроком действия в 1 год. В случае отзыва регистрационных свидетельств НУЦ РК или подписчиков НУЦ РК срок действия заканчивается на момент отзыва. Использование ключевых пар отозванных регистрационных свидетельств НУЦ РК или подписчиков НУЦ РК не допускается.

6.4. АКТИВАЦИОННЫЕ ДАННЫЕ

6.4.1. Генерация и установка данных активации закрытых ключей

Генерация закрытых ключей НУЦ РК сопровождается созданием «секрета» на защищённых носителях ключевой информации в соответствии с процедурой, описанной в пунктом 6.2.2 выше. Использование «секрета» требует двухфакторной аутентификации — использования носителя части секрета и соответствующего уникального PIN-кода. Ответственные участники церемонии генерации закрытых ключей НУЦ РК подбираются исходя из соответствия принципа разделения полномочий и независимости. Данные активации каждой части секрета, вверенного ответственному участнику, вводятся непосредственно самим ответственным участником и не разглашаются остальным ответственным участникам.

Закрытые ключи подписчиков НУЦ РК защищаются паролем, который задаётся самим подписчиком при генерации ключевых пар на удостоверении личности или защищённом носителе. Закрытые ключи подписчиков, сгенерированные на файловую систему, защищаются стандартным паролем «123456», который подписчик должен сменить сразу после генерации ключей.

6.4.2. Защита данных активации

Ответственные участники церемонии генерации ключевых пар НУЦ РК документально соглашаются с ответственностью за хранение доверенной им части секрета и данных активации.

Подписчики НУЦ РК несут ответственность за защиту пароля своего закрытого ключа от разглашения в соответствии с требованиями законодательства Республики Казахстан, требованиями настоящих Правил и Пользовательского соглашения информационной системы Национальный удостоверяющий центр Республики Казахстан для получения государственной услуги «Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан».

6.4.3. Иные аспекты работы с данными активации

Данные активации закрытых ключей НУЦ РК выводятся из использования с применением процедур, защищающих от потери, хищения, модификации, разглашения или несанкционированного использования закрытых ключей, активируемых этими данными. Не подлежащие дальнейшему хранению данные активации выводятся из использования путём физического уничтожения.

6.5. КОНТРОЛИ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

6.5.1. Специальные технические требования компьютерной безопасности

Технические средства НУЦ РК обеспечиваются защитой посредством:

организационно-технических мер обеспечения безопасности (в т.ч. управление доступом, управление обновлениями ПО, антивирусная защита и пр.);

журналирования событий.

6.5.2. Оценка компьютерной безопасности

НУЦ РК использует сертифицированные средства обеспечения компьютерной безопасности, что свидетельствует об успешной оценке высокого уровня безопасности.

НУЦ РК осуществляет периодические оценки уязвимостей в инфраструктуре с оценкой рисков и последующей обработкой рисков.

6.6. КОНТРОЛИ ЖИЗНЕННОГО ЦИКЛА БЕЗОПАСНОСТИ

6.6.1. Контроль развития системы

НУЦ РК разрабатывает собственное программное обеспечение. НУЦ РК использует внутренние контроли для определения требований к обновлениям системы и тестированию.

Система внутренних контролей НУЦ РК предусматривает разделение среды разработки и продуктивной среды, а также разделение полномочий работников в конфликтных ролях разработчиков и администраторов систем.

6.6.2. Контроль управления безопасностью

НУЦ РК обеспечивает функционирование контролей управления безопасностью в соответствии с требованиями стандарта СТ РК ИСО/МЭК 27001.

6.7. КОНТРОЛИ БЕЗОПАСНОСТИ СЕТЕЙ

НУЦ РК обеспечивает безопасность внутренних сетей, а также безопасность данных, передаваемых по внешним сетям. НУЦ РК обеспечивает организационно-технические меры от несанкционированного доступа и атак на свои сети. Политики и процедуры в мероприятиях по контролю безопасности сетей документированы и утверждены, однако не публикуются, поскольку содержат конфиденциальную информацию НУЦ РК.

6.8. ПРОЦЕСС ВРЕМЕННОЙ МАРКИРОВКИ

НУЦ РК подписывает своим специализированным регистрационным свидетельством информацию о дате и точном времени всех журналируемых событий, включая:

дату и точное время событий жизненного цикла регистрационных свидетельств,

дату и точное время выпуска, а также сроки действия списков отозванных регистрационных свидетельств;

дату и точное время ответов служб по проверке статуса регистрационных свидетельств.

7. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК И СОРС

7.1. СТРУКТУРА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДПИСЧИКА НУЦ РК

7.1.1. Структура регистрационного свидетельства подписчика НУЦ РК (физическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = Адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
PublicKey	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш от-	2.5.29.14	–

	крытого ключа по SHA-1		
Authority Key Identifier	Идентификатор ключа центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Неотрекаемость (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Защищенная электронная почта - 1.3.6.1.5.5.7.3.4 Физическое лицо - 1.2.398.3.3.4.1.1
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.3 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики = Текст уведомления Квалификатор: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/rsa.crl URL= http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/d_rsa.crl

			URL= http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.2. Структура регистрационного свидетельства подписчика НУЦ РК (физическое лицо) Национального удостоверяющего центра Республики Казахстан (для аутентификации)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E=1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = адрес электронной почты физического лица (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
PublicKey	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа Центра сер-	2.5.29.35	–

	тификации (4 байта). ID ключа на HSM		
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности клиента - 1.3.6.1.5.5.7.3.2 Физическое лицо-1.2.398.3.3.4.1.1
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.4 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики = Текст уведомления Квалификатор: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/rsa.crl URL= http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/d_rsa.crl URL= http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.3. Структура регистрационного свидетельства подписчика НУЦ РК (юридическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
	Алгоритм хеширования		Алгоритм хеширования ГОСТ 34.311-95
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.4 G=2.5.4.42 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (GOST) (обязательное поле)
Public Key	Значение открытого ключа (512 бит)	1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	ГОСТ 34.310-2004
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш от-	2.5.29.14	–

	крытого ключа по SHA-1		
Authority Key Identifier	Идентификатор ключа Центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Неотрекаемость (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Защищенная электронная почта - 1.3.6.1.5.5.7.3.4 Юридическое лицо - 1.2.398.3.3.4.1.2 Неизвестное использование ключа (OID), где в качестве OID определено множество доступных идентификаторов. **Доступные идентификаторы:** 1.2.398.3.3.4.1.2.1 – Первый руководитель юридического лица, имеющий право подписи 1.2.398.3.3.4.1.2.2 – Лицо, наделенное правом подписи 1.2.398.3.3.4.1.2.3 - Лицо, наделенное правом подписи финансовых документов 1.2.398.3.3.4.1.2.4 – Сотрудник отдела кадров, наделенный правом подтверждать заявки на выпуск регистрационных свидетельств поданные от сотрудников юридического лица 1.2.398.3.3.4.1.2.5 – Сотрудник организации
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.1 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики=Текст уведомления Квалификатор: http://pki.gov.kz/cps
Certificate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_gost.cer [2]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния регистрационно-

			го свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.1.4. Структура регистрационного свидетельства подписчика НУЦ РК (юридическое лицо) Национального удостоверяющего центра Республики Казахстан (для аутентификации)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
	Алгоритм хэширования		sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = Адрес электронный почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа Центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)

			Юридическое лицо (1.2.398.3.3.4.1.2) Неизвестное использование ключа (OID), где в качестве OID определено множесто доступных идентификаторов. **<u>Доступные идентификаторы:</u>** 1.2.398.3.3.4.1.2.1 – Первый руководитель юридического лица, имеющий право подписи 1.2.398.3.3.4.1.2.2 – Лицо, наделенное правом подписи 1.2.398.3.3.4.1.2.3 - Лицо, наделенное правом подписи финансовых документов 1.2.398.3.3.4.1.2.4 – Сотрудник отдела кадров, наделенный правом подтверждать заявки на выпуск регистрационных свидетельств поданные от сотрудников юридического лица 1.2.398.3.3.4.1.2.5 – Сотрудник организации
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики = Текст уведомления Квалификатор: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/rsa.crl URL= http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/d_rsa.crl URL= http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись ЦС (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.5. Структура регистрационного свидетельства подписчика НУЦ РК (ИС Казначейство -Клиент) Национального удостоверяющего центра Республики Казахстан (для подписи)

Поле	Описание	OID, Критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
	Алгоритм хеширования		ГОСТ 34.311-95
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 BUSINESSCATEGORY = 2.5.4.15 DC=0.9.2342.19200300.100.1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) BUSINESSCATEGORY = KS01234 (обязательное поле) DC = ROLE01 (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (GOST) (обязательное поле)
PublicKey	Значение открытого ключа (512 бит)	1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	ГОСТ 34.310-2004
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4	2.5.29.35	–

	байта). ID ключа на HSM		
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Неотрекаемость (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Неизвестное использование ключа (OID), .где в качестве OID определено множесто доступных идентификаторов. **Доступные идентификаторы:** Юридическое лицо -1.2.398.3.3.4.1.2; Информационная система К2 - 1.2.398.5.19.1.2.2.1
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.5.19.1.2.2.1.2 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps
Certificate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_gost.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL = http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/gost.crl URL= http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/d_gost.crl URL= http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.1.6. Структура регистрационного свидетельства подписчика НУЦ РК (ИС Казначейство - Клиент) Национального удостоверяющего центра Республики Казахстан (для аутентификации)

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
	Алгоритм хэширования		sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 BUSINESSCATEGORY= 2.5.4.15 DC=0.9.2342.19200300.100.1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) BUSINESSCATEGORY= KS01234 (обязательное поле) DC = ROLE01 (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Неизвестное использование ключа (OID), где

			в качестве OID определено множесто доступных идентификаторов. **<u>Доступные идентификаторы:</u>** 1.2.398.3.3.4.1.2 – Юридическое лицо; 1.2.398.5.19.1.2.2.1 – Информационная система К2
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.5.19.1.2.2.1.3 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps
Authority Info Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/rsa.crl URL = http://crl1.pki.gov/kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/crl/d_rsa.crl URL = http://crl1.pki.gov.kz/crl/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.7. Структура регистрационного свидетельства RSA ИС «Е-Нотариат» для аутентификации

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
	Алгоритм хэширования		sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное

		CN =2.5.4.3 BUSINESSCATEGORY= 2.5.4.15 DC=0.9.2342.19200300.100 .1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) BUSINESSCATEGORY= KS01234 (обязательное поле) DC = ROLE01 (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Неизвестное использование ключа (OID), где в качестве OID определено множество доступных идентификаторов. Доступные идентификаторы: 1.2.398.3.3.4.1.2 – Юридическое лицо; 1.2.398.5.19.1.2.2.1 – Информационная система К2
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.5.19.1.2.2.1.3

			[1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps
Authority Info Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_rsa.crt [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
CRL Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/rsa.crl URL = http://crl1.pki.gov/kz/rsa.crl
Freshest CRL Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/crl/d_rsa.crl URL = http://crl1.pki.gov.kz/crl/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.8. Структура регистрационного свидетельства ИС «Е-Нотариат» для подписи

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
	Алгоритм хэширования		sha256WithRSAEncryption
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 BUSINESSCATEGORY= 2.5.4.15	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле)

		DC=0.9.2342.19200300.100.1.25 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) BUSINESSCATEGORY= KS01234 (обязательное поле) DC = ROLE01 (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Шифрование ключей (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Неизвестное использование ключа (OID), где в качестве OID определено множество доступных идентификаторов. Доступные идентификаторы: 1.2.398.3.3.4.1.2 – Юридическое лицо; 1.2.398.5.19.1.2.2.1 – Информационная система К2
Certificate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.5.19.1.2.2.1.3 [1,1]Сведения квалификатора политики: Идентификатор квалифи-

			катора политики = CPS Квалификатор: http://pki.gov.kz/cps
Authority Info Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_rsa.crt [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
CRL Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/rsa.crl URL = http://crl1.pki.gov/kz/rsa.crl
Freshest CRL Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/crl/d_rsa.crl URL = http://crl1.pki.gov.kz/crl/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.9. Структура регистрационного свидетельства пользователя (юридическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи), предназначенного для участия в государственных закупках государств-членов Евразийского экономического союза

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
	Алгоритм хеширования		Алгоритм хеширования ГОСТ 34.311-95
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.4	E = адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обяза-

		G=2.5.4.42 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	тельное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (GOST) (обязательное поле)
Public Key	Значение открытого ключа (512 бит)	1.2.398.3.10.1.1.1.1 с параметрами 1.2.398.3.10.1.1.1.1.1 1.2.398.3.10.1.3.1.1.0	ГОСТ 34.310-2004
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа Центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Неотрекаемость (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Защищенная электронная почта - 1.3.6.1.5.5.7.3.4 Юридическое лицо - 1.2.398.3.3.4.1.2 Использование на электронных площадках, отобранных для проведения аукционов в электронной форме(OID 1.2.643.6.3.1.1). Области использования согласно заявлению клиента: Тип участника: Юридическое лицо (OID 1.2.643.6.3.1.2.1) Тип организации: Участник размещения заказа(OID 1.2.643.6.3.1.3.1) Полномочия (множественный выбор): Администратор организации(OID 1.2.643.6.3.1.4.1) Уполномоченный специалист(OID 1.2.643.6.3.1.4.2) Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)
Ceritifcate Policy	Политика регист-	2.5.29.32	[1]Политика регистрационного свидетельст-

	рационного свидетельства		ва: Идентификатор политики=1.2.398.3.3.2.1 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики=Текст уведомления Квалификатор: http://pki.gov.kz/cps
Certificate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_gost.cer [2]Доступ к сведениям центра сертификации Метод доступа=Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/gost.crl URL=http://crl1.pki.gov.kz/gost.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL=http://crl.pki.gov.kz/d_gost.crl URL=http://crl1.pki.gov.kz/d_gost.crl
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.1.10. Структура регистрационного свидетельства нерезидента (физическое лицо) Национального удостоверяющего центра Республики Казахстан (для подписи), предназначенного для участия в государственных закупках государств-членов Евразийского экономического союза

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Subject	Данные Владельца	E =1.2.840.113549.1.9.1	E = Адрес электронной почты (необязатель-

	регистрационного свидетельства	SERIALNUMBER = 2.5.4.5 SN=2.5.4.5 G=2.5.4.42 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	ное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) SN = Фамилия (необязательное поле) G = Отчество (необязательное поле) CN = Фамилия Имя (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
PublicKey	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Key Usage	Использование ключа	2.5.29.15, critical	Цифровая подпись, Неотрекаемость (c0)
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Защищенная электронная почта - 1.3.6.1.5.5.7.3.4 Физическое лицо - 1.2.398.3.3.4.1.1 Использование на электронных площадках, отобранных для проведения аукционов в электронной форме(OID 1.2.643.6.3.1.1). Области использования согласно заявлению клиента: Тип участника: Физическое лицо (OID 1.2.643.6.3.1.2.2) Тип организации: Участник размещения заказа(OID 1.2.643.6.3.1.3.1) Полномочия (множественный выбор): Администратор организации(OID 1.2.643.6.3.1.4.1) Уполномоченный специалист(OID 1.2.643.6.3.1.4.2) Специалист с правом подписи контракта (OID 1.2.643.6.3.1.4.3)
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=1.2.398.3.3.2.3 [1,1]Сведения квалификатора политики:

			Идентификатор квалификатора политики = CPS Квалификатор: http://pki.gov.kz/cps [1,2]Сведения квалификатора политики: Идентификатор квалификатора политики = Текст уведомления Квалификатор: http://pki.gov.kz/cps
Ceritifcate Authority Information Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/rsa.crl URL= http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL= http://crl.pki.gov.kz/d_rsa.crl URL= http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (2048 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.11. Структура регистрационного свидетельства SSL физического лица Национального удостоверяющего центра Республики Казахстан

Поле	**Описание**	**OID, критичность**	**Содержание**
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption

Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER = 2.5.4.5 SN=2.5.4.4 CN =2.5.4.3 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = Адрес электронной почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) CN = Доменное имя (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Extended Key Usage	Расширенное использование ключа	2.5.29.37	Проверка подлинности сервера (1.3.6.1.5.5.7.3.1) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Неизвестное использование ключа (OID), где в качестве OID определено множество доступных идентификаторов. **Доступные идентификаторы:** 1.2.398.3.3.4.1.1 – Физическое лицо
Subject Alternative Name	Дополнительное имя субъекта	2.5.29.17	DNS-имя=Доменное имя-1 DNS-имя= Доменное имя-2 DNS-имя= N (необязательное поле)
Authority Info Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертифи-

			кации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	1]Политика сертификата: Идентификатор политики= 1.2.398.3.3.2.5 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: http://pki.gov.kz/cps
Crl Distribution Points	Точки распространения списков отзыва	2.5.29.31	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/rsa.crl URL = http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/d_rsa.crl URL = http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.12. Структура регистрационного свидетельства SSL юридического лица Национального удостоверяющего центра Республики Казахстан

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
Serial Number	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
Validity from	Время начала срока действия	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Validity to	Время окончания срока действия	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Subject	Данные Владельца регистрационного свидетельства	E =1.2.840.113549.1.9.1 SERIALNUMBER =2.5.4.5 SN=2.5.4.4 CN =2.5.4.3 OU=2.5.4.11 O=2.5.4.10 L=2.5.4.7 S=2.5.4.8 C=2.5.4.6	E = Адрес электронный почты (необязательное поле) SERIALNUMBER = IIN012345678910 (обязательное поле) CN = Доменное имя (обязательное поле) OU = BIN012345678910 (обязательное поле) O = Наименование организации (обязательное поле) L = Город (обязательное поле) S = Область (обязательное поле) C = KZ (обязательное поле)
Public Key	Значение открытого ключа (2048 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Extended Key Usage	Расширенное ис-	2.5.29.37	Проверка подлинности сервера

	пользование ключа		(1.3.6.1.5.5.7.3.1) Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Неизвестное использование ключа (OID), где в качестве OID определено множество доступных идентификаторов. **Доступные идентификаторы:** 1.2.398.3.3.4.1.2 – Юридическое лицо
Subject Alternative Name	Дополнительное имя субъекта	2.5.29.17	DNS-имя=Доменное имя-1 DNS-имя= Доменное имя-2 DNS-имя= N (необязательное поле)
Authority Info Access	Доступ к информации о центрах сертификации	1.3.6.1.5.5.7.1.1	[1]Доступ к сведениям центра сертификации Метод доступа = Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL = http://pki.gov.kz/cert/pki_rsa.cer [2]Доступ к сведениям центра сертификации Метод доступа = Протокол определения состояния регистрационного свидетельства через сеть (1.3.6.1.5.5.7.48.1) Дополнительное имя: URL=http://ocsp.pki.gov.kz/ocsp/
Subject Key Identifier	Идентификатор ключа субъекта (20 байтов). Хэш открытого ключа по SHA-1	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	1]Политика сертификата: Идентификатор политики= 1.2.398.3.3.2.5 [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики=CPS Квалификатор: http://pki.gov.kz/cps
Crl Distribution Points	Точки распространения списков отзы-	2.5.29.31	[1]Точка распределения списка отзыва (CRL)

	ва		Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/rsa.crl URL = http://crl1.pki.gov.kz/rsa.crl
Freshest Crl Distribution Points	Новейший CRL	2.5.29.46	[1]Новейший CRL Имя точки распространения: Полное имя: URL = http://crl.pki.gov.kz/d_rsa.crl URL = http://crl1.pki.gov.kz/d_rsa.crl
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.13. Информация о списке отозванных регистрационных свидетельств RSA Национального удостоверяющего центра Республики Казахстан

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V2
Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
This Update	Время издания	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Next Update	Следующее обновление	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Дополнительные поля регистрационного свидетельства в формате X.509			
Number CRL	Номер CRL	2.5.29.20	Последовательно увеличивающийся номер
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–

Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.14. Информация о списке отозванных регистрационных свидетельств GOST Национального удостоверяющего центра Республики Казахстан

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V2
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (GOST) (обязательное поле)
This Update	Время издания	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Next Update	Следующее обновление	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Дополнительные поля регистрационного свидетельства в формате X.509			
Number CRL	Номер CRL	2.5.29.20	Последовательно увеличивающийся номер
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.1.15. Информация о списке отозванных регистрационных свидетельств RSA (Delta CRL) Национального удостоверяющего центра Республики Казахстан

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V2

Signature Algorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле) CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (RSA) (обязательное поле)
This Update	Время издания	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Next Update	Следующее обновление	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Дополнительные поля регистрационного свидетельства в формате X.509			
Number CRL	Номер CRL	2.5.29.20	Последовательно увеличивающийся номер
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Freshest CRL	Идентификатор разностного CRL	2.5.29.46, critical	–
Digital Signature	Цифровая подпись ЦС (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.16. Информация о списке отозванных регистрационных свидетельств GOST (Delta CRL) Национального удостоверяющего центра Республики Казахстан

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V2
Signature Algorithm	Алгоритм подписи	1.2.398.3.10.1.1.1.2	ГОСТ 34.310-2004
Issuer	Данные издателя регистрационного свидетельства	C=2.5.4.6 L=2.5.4.7 S=2.5.4.8 O=2.5.4.10 CN =2.5.4.3	C = KZ (обязательное поле) L = АСТАНА (обязательное поле) S = АСТАНА (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)

			CN = ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҒЫ (GOST) (обязательное поле)
This Update	Время издания	UTC TIME	Действителен с: YYMMDDHHMMSSZ GMT
Next Update	Следующее обновление	UTC TIME	Действителен по: YYMMDDHHMMSSZ GMT
Дополнительные поля регистрационного свидетельства в формате X.509			
Number CRL	Номер CRL	2.5.29.20	Последовательно увеличивающийся номер
Authority Key Identifier	Идентификатор ключа ЦС (4 байта). ID ключа на HSM	2.5.29.35	–
Freshest CRL	Идентификатор разностного CRL	2.5.29.46, critical	–
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.2. ПРОФИЛЬ OCSP

Версия службы OCSP, используемая НУЦ РК для проверки статуса регистрационного свидетельства, соответствует версии 1 рекомендаций RFC 2560.

Расширения, обрабатываемые сервисом OCSP, а также их критичность, соответствует рекомендациям RFC 2560.

8. АУДИТ СООТВЕТСТВИЯ

Внутренняя контрольная среда НУЦ РК проверяется на соответствие требованиям международного стандарта WebTrust. Аудит осуществляются независимыми аудиторскими компаниями, лицензированными владельцем стандарта WebTrust.

8.1. ПЕРИОДИЧНОСТЬ И ОСНОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУДИТА

Аудит внутренней контрольной среды НУЦ РК на соответствие требованиям международного стандарта WebTrust (внешний аудит) проводится не реже чем раз в год.

В соответствии с требованиями международного стандарта WebTrust, РГП «ГТС» планирует приобретение услуг внешнего аудита у независимых аудиторских организаций, соответствующих требованиям, изложенным в пункте 8.2 ниженастоящих Правил.

КСИИ МИР РК осуществляет государственный закуп услуг по проведению сертификационного аудита на соответствие требованиям международного стандарта WebTrust.

8.2. АУДИТОРЫ И ИХ КВАЛИФИКАЦИЯ

Аудит внутренней контрольной среды НУЦ РК на соответствие требованиям международного стандарта WebTrust осуществляются независимыми аудиторскими организациями, имеющими лицензию от владельца международного стандарта WebTrust на проведение сертификационного аудита на соответствие международному стандарту WebTrust . Лицензия от владельца стандарта WebTrust выдается после проверки квалификации аудиторской организации.

8.3. ОТНОШЕНИЯ МЕЖДУ НУЦ РК И АДИТРСКИМИ ОРГАНИЗАЦИЯМИ

Аудиторские организации, осуществляющие аудит внутренней контрольной среды НУЦ РК на соответствие требованиям международного стандарта WebTrust, являются независимыми от РГП «ГТС» и КСИИ МИР РК.

8.4. ЗАДАЧИ АУДИТА

Аудит внутренней контрольной среды НУЦ проводится в соответствии с международным стандартом WebTrust для удостоверяющих центров. В объём проверок входят следующие разделы международного стандарта WebTrust:

1) раскрытие бизнес-практик НУЦ РК:

управление политикой применения регистрационных свидетельств НУЦ РК;

управление инструкцией по применению регистрационных свидетельств НУЦ РК.

2) контроли среды НУЦ РК:

управление информационной безопасностью;

классификация активов и управление ими;
безопасность персонала;
управление физической безопасностью;
управление деятельностью НУЦ РК;
управление доступом;
управление разработкой и поддержкой систем;
управление непрерывностью бизнеса;
мониторинг и управление соответствием требованиям;
протоколирование.
3) контроли жизненного цикла ключей НУЦ РК:
генерация ключей НУЦ РК;
хранение, резервное копирование и восстановление ключей НУЦ РК;
распространение публичных ключей НУЦ РК;
использование ключей НУЦ РК;
архивирование и уничтожение ключей НУЦ РК;
контроли компрометации ключей НУЦ РК;
управление жизненным циклом СКЗИ НУЦ РК.
4) контроли жизненного цикла ключей подписчиков НУЦ РК:
услуги НУЦ РК по генерации ключей подписчиков НУЦ РК;
требования по управлению ключами подписчиков НУЦ РК.
5) контроли управления жизненным циклом регистрационных свидетельств НУЦ РК:
регистрация подписчиков;
выдача регистрационных свидетельств НУЦ РК;
распространение регистрационных свидетельств НУЦ РК;
отзыв регистрационных свидетельств НУЦ РК;
проверка регистрационных свидетельств НУЦ РК.

8.5. МЕРЫ, ПРЕДПРИНИМАЕМЫЕ ПРИ ВЫЯВЛЕНИИ НЕДОСТАТКОВ И НАРУШЕНИЙ

По результатам проверок внутренней контрольной среды НУЦ РК на соответствие требованиям международного стандарта WebTrust, лицензированные аудиторские организации предоставляют в КСИИ МИР РК итоговый отчёт, содержащий перечень выявленных недостатков или нарушений, а также описание связанных с недостатками или нарушениями рисков и рекомендации по их устранению. На основании итогового отчёта по аудиту, ответственные работники РГП «ГТС» составляют план устранения недостатков и нарушений с указанием сроков выполнения, ответственных лиц и результатов выполнения плана. План утверждается ответственными лицами КСИИ МИР РК. Контроль за исполнением плана устранения недостатков и нарушений осуществляется КСИИ МИР РК.

НУЦ РК предоставляет КСИИ МИР РК информацию о ходе устранения выявленных недостатков в соответствии с планом устранения недостатков и нарушений. НУЦ РК предоставляет независимым лицензированным аудиторам информацию об устранении ранее выявленных недостатков при следующей ежегодной проверке внутренней контрольной среды НУЦ РК.

9. ПРАВОВАЯ ДЕЯТЕЛЬНОСТЬ

9.1. ОПЛАТА УСЛУГ

РГП «ГТС» и РГП «ЦОН» не взимают платы за предоставление государственной услуги.

9.2. ФИНАНСОВАЯ ОТВЕТСТВЕННОСТЬ

9.2.1. Страховое покрытие

НУЦ РК не представляет страхового покрытия никому из участников ИОК НУЦ РК.

9.2.2. Иная финансовая ответственность

Не предусмотрено.

9.3. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ НУЦ РК

9.3.1. Конфиденциальная информация НУЦ РК

НУЦ РК в процессе своей деятельности обрабатывает, получает, использует и хранит конфиденциальную информацию, при этом НУЦ РК принимает все необходимые меры по ее защите в соответствии с действующим законодательством Республики Казахстан. Информация НУЦ РК, не рассматриваемая в качестве конфиденциальной

К конфиденциальной информации не относиться публичная информация указанная в разделе _____.

9.3.2. Ответственность по защите конфиденциальной информации НУЦ РК

НУЦ РК несёт ответственность по защите обрабатываемой, получаемой, используемой и хранящейся конфиденциальной информации в соответствии с действующим законодательством Республики Казахстан.

9.4. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ ПОДПИСЧИКОВ НУЦ РК

9.4.1. Обеспечение конфиденциальности НУЦ РК персональных данных подписчиков НУЦ РК

НУЦ РК обеспечивает защиту персональных данных подписчиков НУЦ РК в соответствии с действующим законодательством Республики Казахстан.

В случае прекращения деятельности НУЦ РК обязан за тридцать дней до прекращения своей деятельности проинформировать об этом всех участников ИОК НУЦ РК и уполномоченный орган.
При прекращении деятельности НУЦ РК выданные им регистрационные свидетельства и соответствующие ключи электронной цифровой подписи, сведения о регистрационных свидетельств подписчиков НУЦ РК передаются в другие удостоверяющие центры по согласованию с подписчиками НУЦ РК регистрационного свидетельства.

По истечении срока, регистрационные свидетельства подписчиков НУЦ РК и соответствующие ключи ЭЦП, не переданные в другие удостоверяющие центры, прекращают свое действие и подлежат хранению в соответствии с законодательством Республики Казахстан.

9.4.2. Информация, рассматриваемая в качестве персональных данных подписчиков НУЦ РК

НУЦ РК рассматривает в качестве персональных данных информацию о подписчике НУЦ РК указанной в регистрационных свидетельствах подпсичиков НУЦ РК.

9.4.3. Информация, не рассматриваемая в качестве персональных данных подписчиков НУЦ РК

НУЦ РК не рассматривает в качестве персональных данных информацию, содержащуюся в регистрационных свидетельствах подписчиков НУЦ РК, а также иную информацию, подлежащую обязательному опубликованию в соответствии с действующим законодательством Республики Казахстан.

9.4.4. Ответственность за защиту персональных данных подписчиков НУЦ РК

НУЦ РК несёт ответственность по защите обрабатываемой, получаемой, используемой и хранящейся персональных данных подписчика НУЦ РК в соответствии с действующим законодательством Республики Казахстан.

9.4.5. Согласие на использование персональных данных подписчиком НУЦ РК

При подаче заявления на выдачу регистрационного свидетельства НУЦ РК заявитель подтверждает свое согласие на сбор, обработку, использование и хранение персональных данных в соответствии с пользовательским соглашением.

9.4.6. Раскрытие персональных данных подписчиков НУЦ РКправоохранительным и судебным органам

НУЦ РК предоставляет конфиденциальную информацию о персональных данных подписчиков НУЦ РК в правоохранительные и судебные органам в соответствии с действующим законодательством Республики Казахстан.

9.4.7. Другие основания для раскрытия персональных данных подписчиков НУЦ РК

Не применяются.

9.5. ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ

НУЦ РК оставляет за собой права интеллектуальной собственности на регистрационные свидетельства, которые он выдаёт, и на информацию об их статусе. При этом НУЦ РК не запрещает копирование и распространение регистрационных свидетельств на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования регистрационных свидетельств в соответствии с условиями заключенных пользовательских Соглашений. НУЦ РК также не запрещает использование информации о статусе регистрационных свидетельств для выполнения функций доверяющей стороны.

Участники информационных систем, обслуживаемых НУЦ РК, признают право интеллектуальной собственности НУЦ РК на настоящий Регламент и другую документацию НУЦ РК, регламентирующую деятельность УЦ.

Заявители на выдачу регистрационных свидетельств сохраняют все свои права на все торговые и тому подобные марки и имена, содержащиеся в заявлениях на выдачу регистрационных свидетельств и отличительные (DN-) имена в выпущенных регистрационных свидетельствах.

Ключевые пары, которые соответствуют регистрационным свидетельствам, выпущенным НУЦ РК, составляют собственность (в том числе интеллектуальную) соответствующих участников ИОК НУЦ РК независимо от физических носителей, на которых хранятся эти ключевые пары и которыми они защищаются. В частности, открытые ключи, регистрационных свидетельств и части секрета закрытых ключей НУЦ РК, являются собственностью (в том числе интеллектуальной) НУЦ РК.

9.6. ГАРАНТИИ

9.6.1. Гарантии НУЦ РК

НУЦ РК гарантирует предоставление государственной услуги, за исключением объективных причин, ложных срабатываний и производственной необходимости.

9.6.1. Гарантии РГП ЦОН

РГП «ЦОН» гарантирует:

Внесение операторами ЦР достоверной информации заявлениях на выдачу регистрационных свидетельствах НУЦ РК;

отсутствие в заявлениях на выдачу регистрационных свидетельств случайных ошибок;

своевременное информирование заявителей на выдачу регистрационных свидетельств об условиях, обязанностях и ответственности, которые влечёт получение регистрационного свидетельства НУЦ РК.

9.6.2. Гарантии и обязательства подписчиков НУЦ РК

Подписчик НУЦ РК гарантирует использования регистрационного свидетельства НУЦ РК в соответствии с настоящими Правилами и действующим законодательством Республики Казахстан.

9.6.3. Гарантии доверяющих сторон

Доверяющие стороны гарантируют использования регистрационного свидетельства НУЦ РК в соответствии с настоящими Правилами и действующим законодательством Республики Казахстан

Не предусмотрено.

9.7. СРОК ДЕЙСТВИЯ И ПОРЯДОК ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ

9.7.1. Вступление в силу

Настоящие Правила вступают в силу с момента опубликования на интернет-ресурсе НУЦ РК

9.7.2. Прекращение действия

Настоящие Правила прекращают действия с момента опубликования новой версией Правил в течение функционирования НУЦ РК. Замена новой версией Правил осуществляется в соответствии с пунктом **Ошибка! Источник ссылки не найден.**.

9.7.3. Правовые последствия прекращения действия

С момента прекращения действия настоящих Правил участники ИОК НУЦ РК остаются связанными условиями последней версии Правил по всем регистрационным свидетельствам НУЦ РК до момента истечения периода действия каждого из регистрационных свидетельств подписчиков НУЦ РК.

9.8. ИНДИВИДУАЛЬНЫЕ УВЕДОМЛЕНИЯ И ВЗАИМОДЕЙСТВИЕ С УЧАСТНИКАМИ

НУЦ РК использует все доступные методы официального уведомления участников ИОК НУЦ РК.

9.9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

Споры возникшие в ходе деятельности или предоставление государственной услуги, должны урегулироваться по соглашению сторон и стороны должны принять все усилия для решение возникших споров. Неурегулированные споры рассматриваются в судебном порядке г. Астана в соответствии с законодательством Республики Казахстан.

9.10. ПРОЧИЕ ПОСТАНОВЛЕНИЯ

9.10.1. Полнота соглашения

Не оговаривается.

9.10.2. Передача прав

Не предусматривается.

9.10.3. Делимость

В случае если часть положений настоящих Правил будет признана неосуществимой судом или уполномоченным государственным органом, остальная ее часть сохраняет силу.

9.10.4. Право применение (адвокатские компенсации и отказ от прав)

Не оговаривается.

9.10.5. Форс-мажор

Не оговаривается.

9.11. ДРУГИЕ ПОЛОЖЕНИЯ

Не предусматриваются.