РЕСПУБЛИКАНСКОЕ ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ НА ПРАВЕ ХОЗЯЙСТВЕННОГО ВЕДЕНИЯ «ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ СЛУЖБА» МИНИСТЕРСТВА ИНФОРМАЦИИ И КОММУНИКАЦИЙ РЕСПУБЛИКИ КАЗАХСТАН

«УТВЕРЖДАЮ»

Директор
РГП «Государственная техническая служба»
Министерства информации и коммуникаций
Республики Казахстан

_____ Е.К. Есмамбетов
«09» сентября 2016 г.

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

Версия 2.0

Астана, 2016 г.

КОНТРОЛИ ВЕРСИЙ

№	Статус	Дата	Автор	Описание изменение
2.0	С внесенными поправками	18 октября 2016 года	Кенжебулатов Б. С.	приказ директора РГП «ГТС» от 18 октября 2016 года № 01-04/252 «О внесении изменений и дополнения в приказ директора РГП «ГТС» от 9 сентября 2016 года № 01-04/208 «Об утверждении документов Корневого удостоверяющего центра Республики Казахстан»
2.0	Действующие	9 сентября 2016 года	Кенжебулатов Б. С.	Правила приведены в соответствие с требованиями международного стандарта WebTrust
1.0	Утратившие силу	26 июня 2015 года	Кенжебулатов Б. С.	-

Содержание

1. ВВЕДЕНИЕ

Корневой удостоверяющий центр Республики Казахстан (далее — КУЦ РК) создан в целях осуществления подтверждения принадлежности и действительности открытых ключей электронной цифровой подписи (далее — ЭЦП) удостоверяющих центров (далее — УЦ). Для этих целей КУЦ РК обеспечивает выдачу (переподчинение) регистрационных свидетельств аккредитованных УЦ в соответствии с Постановлением Правительства Республики Казахстан от 19 ноября 2010 года № 1222 «Об утверждении Правил проведения аккредитации удостоверяющих центров».

КУЦ РК осуществляет деятельность в соответствии со следующими нормативными правовыми актами Республики Казахстан, внутренними документами 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 24 ноября 2015 года «Об информатизации»;

3) приказ Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года № 1184 «Об утверждении Типового положения удостоверяющего центра»;

4) приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 26 июня 2015 года № 727 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром Республики Казахстан, удостоверяющим центром государственных органов и национальным удостоверяющим центром Республики Казахстан»;

5) постановление Правительства Республики Казахстан от 19 ноября 2010 года № 1222 «Об утверждении Правил проведения аккредитации удостоверяющих центров»;

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

7) политика применения регистрационных свидетельств КУЦ РК.

КУЦ РК выдает регистрационные свидетельства только подчинённым УЦ КУЦ РК при условии их аккредитации уполномоченным органом. КУЦ РК не выдает регистрационные свидетельства конечным пользователям, а лишь сертифицирует подчиненные УЦ.

1.1. ПОНЯТИЯ И АББРЕВИАТУРЫ

В настоящей Политике используются следующие понятия:

№	Термин	Определение
1.	Активы	Ресурсы РГП ГТС, направленные на обеспечения непрерывности работы КУЦ РК
2.	Внутренняя контрольная среда	Совокупность контролей процессов КУЦ РК
3.	Журнал работ КУЦ РК	Файл с записями о событиях ИС КУЦ РК в хронологическом порядке
4.	Закрытый ключ ЭЦП	последовательность электронных цифровых символов, известная владельцу регистрационных свидетельств и предназначенная для создания электронной цифровой подписи с использованием средств ЭЦП
5.	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)
6.	Интернет-ресурс КУЦ РК	Интернет-ресурс КУЦ РК www.root.gov.kz
7.	Ключевая пара	Набор, состоящий из двух ключей: закрытого (секретного) ключа и открытого ключа
8.	Открытый ключ ЭЦП	Последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности ЭЦП в электронном документе
9.	Регистрационное свидетельство	Документ на бумажном носителе или электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия ЭЦП требованиям, установленным нормативно-правовыми актами Республики Казахстан

В настоящей Политике используются следующие аббревиатуры:

№	Аббревиатура	Определение
1.	TSP	(Time Stamp Protocol – протокол штампа времени) Криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени
2.	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»)
3.	ИОК	(Инфраструктура Открытых Ключей) 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
4.	КУЦ РК	(Корневой Удостоверяющий Центр Республики Казахстан) Удостоверяющий центр, осуществляющий подтверждение принадлежности и действительности открытых ключей электронной цифровой подписи удостоверяющих центров
5.	МИК РК	(Министерство информации и коммуникаций Республики Казахстан)
6.	НУЦ РК	(Национальный Удостоверяющий Центр Республики Казахстан) Удостоверяющий центр, обслуживающий участников «электронного правительства», государственных и негосударственных информационных систем
7.	РГП ГТС	(Республиканское Государственное Предприятие на праве хозяйственного ведения «Государственная техническая служба» Министерства информации и коммуникаций Республики Казахстан)
8.	СОРС	(Список Отозванных Регистрационных Свидетельств) Перечень всех регистрационных свидетельств подписчиков КУЦ РК, отозванных на момент выпуска СОРС
9.	УЦГО	(Удостоверяющий Центр Государственных Органов Республики Казахстан) Удостоверяющий центр, обслуживающий государственные органы, должностных лиц государственных органов в информационных системах государственных органов Республики Казахстан
10.	ЭЦП	(Электронная Цифровая Подпись) Набор электронных цифровых символов, созданный средствами электронной цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.

1.2. ОБЗОР

Настоящие правила применения регистрационных свидетельств КУЦ РК (далее — Правила) регламентируют деятельность КУЦ РК и детализируют для подчинённых УЦ Политику применения регистрационных свидетельств КУЦ РК (далее - Политика). Настоящие Правила устанавливают нормы, реализуемые КУЦ РК при обеспечении сервисов, определенных Политикой.

Настоящие Правила составлены в соответствии со следующими международными 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 со стандартом X.509 «Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework» (далее — «RFC 3647»).

В соответствии с вышеуказанными стандартами, настоящие Правила состоят из 9 разделов, которые описывают практики предоставления услуг в отношении выдачи (переподчинения) и отзыва регистрационных свидетельств подчинённых УЦ, а также контроли безопасности, применяемые для защиты ИОК КУЦ РК. В целях сохранения соответствия структуры Правил принципам и критериям международного стандарта WebTrust и рекомендациям RFC 3647 секции, не применимые к практикам ИОК КУЦ РК, содержат пометку «не применимо» или «не оговаривается».

Настоящие Правила описывают деятельность КУЦ РК, применяемые в отношении регистрационных свидетельств КУЦ РК и регистрационных свидетельств подчинённых УЦ в соответствии требованиями, установленными в Политике применения регистрационных свидетельств КУЦ РК. Практики КУЦ 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 Корневого удостоверяющего центра Республики Казахстан.

Версия документа: 2.0

Введены в действие приказом директора РГП «ГТС» №01-04/208 от 9 сентября 2016 года.

Действующая версия настоящих Правил публикуется на Интернет-ресурсе КУЦ РК.

1.4. УЧАСТНИКИ ИОК КУЦ РК

1.4.1. КУЦ РК

КУЦ РК является удостоверяющим центром, который выдает (переподчиняет) регистрационные свидетельства аккредитованным УЦ, предназначенные для использования в соответствии с положениями п. 1.5 настоящих Правил.

КУЦ РК осуществляет деятельность, которая непосредственно связана с СУЦ РК, а именно:

- получение и обработка запросов на выдачу (переподчинение) и отзыв регистрационных свидетельств аккредитованных УЦ;
- выдача (переподчинение) и отзыв регистрационных свидетельств аккредитованных и подчинённых УЦ;
- публикация и поддержка списков отозванных подчинённых регистрационных свидетельств подчинённых УЦ (далее — СОРС);
- поддержка регистра регистрационных свидетельств;
- хранение регистрационных свидетельств.

1.4.2. Аккредитованные УЦ

УЦ, официально признанные уполномоченным органом в сфере информатизации компетентным УЦ в оказании услуг в соответствии с законодательством Республики Казахстан.

1.4.3. Подчинённые УЦ

Подчинёнными УЦ считаются аккредитованные УЦ.

1.4.4. Подписчики подчинённых УЦ

Подписчик подчинённого УЦ — владелец регистрационного свидетельства, физическое или юридическое лицо, на имя которого подчинённый УЦ выдал регистрационное свидетельство подписчика, правомерно владеющее закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве подписчика.

1.4.5. Доверяющие стороны

Доверяющая сторона — субъект, который предпринимает действия, основываясь на регистрационном свидетельстве подписчика, выпущенном подчинённым УЦ. Доверяющая сторона может быть подписчиком подчинённого УЦ или подчинённым УЦ.

1.4.6. СУЦ РК

В целях создания основы единого пространства доверия между участниками информационного обмена в Республике Казахстан функционирует инфраструктура системы УЦ РК. Участниками СУЦ РК являются:

КУЦ РК;

подчинённые УЦ, в том числе:

- НУЦ РК;
- УЦ ГО РК;

владельцы регистрационных свидетельств подчинённых УЦ.

СУЦ РК поддерживает иерархическую архитектуру доверия, основные положения которой заключаются в следующем:

- на вершине иерархии СУЦ РК находится КУЦ РК, который выпускает самоподписанные корневые

регистрационные свидетельства КУЦ РК;

- КУЦ РК регистрирует (переподчиняет) корневые регистрационные свидетельства для аккредитованных УЦ;
- подчинённые УЦ выпускают регистрационные свидетельства для своих подписчиков;
- участники СУЦ РК имеют открытый ключ ЭЦП КУЦ РК и соответствующие регистрационные свидетельства.

Участники СУЦ РК при получении электронного документа, содержащего регистрационное свидетельство подписывающей стороны, осуществляют его проверку на подтверждение принадлежности и действительности открытого ключа ЭЦП путём проверки:

- ЭЦП в электронном документе — проверка производится с использованием СКЗИ УЦ путём использования открытого ключа, который содержится в регистрационном свидетельстве подписывающей стороны;
- подлинности регистрационного свидетельства — подлинность регистрационного свидетельства подтверждается подписанным закрытым ключом ЭЦП следующего регистрационного свидетельства в построенной цепочке регистрационных свидетельств;
- построения корректной цепочки от проверяемого регистрационного свидетельства до регистрационного свидетельства КУЦ РК, с учётом промежуточных регистрационных свидетельств подчинённых УЦ;
- регистрационного свидетельства на отзыв (аннулирование) (CORC);
- регистрационного свидетельства на отзыв (аннулирование) в режиме онлайн;
- номера политики регистрационного свидетельства и разрешённых способах его использования;
- метки времени;
- области использования ключа.

1.4.7. Другие участники

Не применимо.

1.5. ПРИМЕНЕНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

1.5.1. Применение регистрационных свидетельств подчинённых УЦ

Регистрационные свидетельства подчинённых УЦ применимы для следующих целей:
выпуск и отзыв регистрационных свидетельств для заявителей подчинённых УЦ;
подтверждение принадлежности и действительности открытого ключа ЭЦП путём проверки.

1.5.2. Требования к применению регистрационных свидетельств подчинённых УЦ

Применение регистрационных свидетельств подчинённых УЦ не должны противоречить действующему законодательству Республики Казахстан, а также требованиям настоящих Правил.

Регистрационные свидетельства подчинённых УЦ запрещается применять:

- после окончания срока действия регистрационного свидетельства КУЦ РК и подчинённого УЦ;
- в случае отзыва регистрационного свидетельства КУЦ РК и подчинённого УЦ;
- в случае подозрения на компрометацию закрытого ключа, удостоверенного регистрационным свидетельством подчинённого УЦ;
- в случае обнаруженной компрометации закрытого ключа, удостоверенного регистрационным свидетельством подчинённого УЦ;
- в случаях, противоречащих пункту 1.5.1 настоящего раздела.

1.6. УПРАВЛЕНИЕ НАСТОЯЩИМИ ПРАВИЛАМИ

1.6.1. Организация, администрирующая документ

РГП «ГТС»

1.6.2. Контактное лицо

Главный специалист сектора трансграничного и межведомственного взаимодействия Службы инфраструктуры открытых ключей Департамента инфраструктурных решений РГП «ГТС» - Кенжебулатов Бауржан Сайранбекович, тел. 55-99-99 (Вн. 398), моб. 8(707)-722-11-33, email – b_kenzhebulatov@sts.kz

1.6.3. Лицо, определяющее соответствие УЦ требованиям правил

Директор РГП «ГТС» - Есмамбетов Ерлан Кожабергенович, тел. 55-99-22, email – info@sts.kz

Директор РГП «ГТС» ответственен за подтверждение соответствия настоящих Правил Политике применения регистрационных свидетельств КУЦ РК (certificate policy).

Директор РГП «ГТС» ответственен за определение общих требований к инфраструктуре открытых ключей, к настоящим Правилам.

1.6.4. Процедура квалифицирования регламента

Разработка, поддержка и обновление настоящих Правил осуществляется РГП «ГТС». Реквизиты:

- юридический адрес: Республика Казахстан, 010000, г. Астана, ул. Жирентаева 1/1;
- фактический адрес: Республика Казахстан, 010000, г. Астана, ул. Куйши Дина 16;
- директор Департамента инфраструктурных решений РГП «ГТС», info@pki.gov.kz, телефон 55 99 99 (399)

Изменения или дополнения в настоящие Правила вносятся после их проверки на соответствие Политике применения регистрационных свидетельств КУЦ РК. Предложения по изменениям или дополнениям в Правила вносятся ответственными работниками КУЦ РК и утверждаются приказом директора РГП «ГТС».

Утверждённые изменённые или дополненные Правила публикуются на Интернет-ресурсе КУЦ 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 утратившие силу версии Правил также остаются опубликованными на Интернет-ресурсе КУЦ РК. Все утратившие силу версии Правил снабжаются пометкой с указанием дат утверждения Правил и ссылкой на действующую версию Правил.

2. ОТВЕТСТВЕННОСТЬ В ОТНОШЕНИИ ПУБЛИКАЦИИ И ХРАНЕНИЯ

2.1. ХРАНИЛИЩЕ И ДОСТУПНОСТЬ ПУБЛИЧНОЙ ИНФОРМАЦИИ

КУЦ РК обеспечивает публичную доступность 24 часа в сутки, 7 дней в неделю следующих материалов на официальном Интернет-ресурсе КУЦ РК:

- корневое регистрационное свидетельство КУЦ РК по алгоритму RSA доступное по адресу http://root.gov.kz/cert/root_rsa.cer;
- корневое регистрационное свидетельство КУЦ РК по алгоритму ГОСТ, доступное по адресу http://root.gov.kz/cert/root_gost.cer;
- объектные идентификаторы Республики Казахстан;
- СОРС (см. п. 2.2.1. ниже);
- Политика применения регистрационных свидетельств КУЦ РК;
- настоящие Правила.

Срок хранения СОРС в регистре регистрационных свидетельств составляет не менее пяти лет, при этом отозванные регистрационные свидетельства находятся в СОРС до даты истечения срока действия регистрационного свидетельства.

По истечении срока хранения СОРС в регистре регистрационных свидетельств, СОРС (устаревшие) поступают на архивное хранение в порядке, установленном действующим законодательством Республики Казахстан.

2.2. ПУБЛИКАЦИЯ ИНФОРМАЦИИ О РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВАХ

2.2.1. СОРС подчинённых УЦ

СОРС КУЦ РК предоставляется в электронной форме и формате, определённом рекомендациями RFC 5280 (Certificate and Certificate Revocation List (CRL) Profile) и настоящими Правилами. КУЦ РК публикует следующие виды СОРС:

- СОРС для регистрационных свидетельств RSA, доступные по адресу: http://crl.root.gov.kz/rsa.crl;
- СОРС для регистрационных свидетельств ГОСТ, доступные по адресу: http://crl.root.gov.kz/gost.crl.

2.3. ПЕРИОД ПУБЛИКАЦИИ ИНФОРМАЦИИ

СОРС выпускается и публикуется не реже, чем 1 раз в 35 суток. Срок действия СОРС составляет не более 35 суток.

2.4. КОНТРОЛЬ ДОСТУПА К ПУБЛИЧНОЙ ИНФОРМАЦИИ

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

КУЦ РК публикует регистрационные свидетельства, которые он выпустил. В случае отзыва регистрационного свидетельства подчиненного УЦ КУЦ РК удаляет это регистрационное свидетельство из действующего хранилища.

В любое время на официальном Интернет – ресурсе КУЦ РК доступны актуальные версии:

- Политики;
- Правила;
- СОРС;
- Нормативные правовые акты в области электронного документа и электронной цифровой подписи.

3. ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1. ПРИСВАИВАНИЕ ИМЁН

3.1.1. Типы имён подчиненных УЦ

Регистрационное свидетельство подчинённого УЦ содержит 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:

Компонент	Значение	Длина	Обязательность
Наименование страны «countryName»	KZ	2 символа	Обязательное
Административно-территориальная единица «State»	Область, город республиканского значения, в котором находится подчинённый УЦ	Не более 32 символов	Обязательное
Местонахождение «Locality»	Город, в котором находится подчинённый УЦ	Не более 16 символов	Обязательное
Адрес электронной почты (E)	Адрес электронной почты подчинённого УЦ	Не более 32 символов	Обязательное
Персональное имя «commonName»	Наименование подчинённого УЦ	Не более 64 символов	Обязательное

3.1.2. Необходимость использования персональных данных в DN-имени

КУЦ РК выдает (переподчиняет) регистрационные свидетельства подчинённых УЦ, которые содержат персональные данные в DN-имени, позволяющие идентифицировать подчиненного УЦ и область применения регистрационного свидетельства подчиненного УЦ.

3.1.3. Анонимность или использование псевдонимов подчинённых УЦ

Анонимность подчинённых УЦ и использование псевдонимов подчинённых УЦ 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.

3.1.5. Необходимость использования уникальных DN-имён

Каждому уникальному подчинённому УЦ должно соответствовать уникальное имя в поле «Subject» регистрационного свидетельства.

3.1.6. Распознавание, аутентификация и роль торговых марок

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

Использование подчинёнными УЦ в отличительном поле «Subject» торговых марок в названиях юридических лиц осуществляется в соответствии с законодательством Республики Казахстан.

3.2. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ЗАЯВИТЕЛЕЙ ПРИ ВЫДАЧЕ (ПЕРЕПОДЧИНЕНИЮ) РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ АККРЕДИТОВАННЫХ УЦ

Идентификация аккредитованных УЦ осуществляется на основании заявления на регистрацию (переподчинение) регистрационного свидетельства, аккредитованного УЦ.

Подчинённые УЦ, обладающие действующим регистрационным свидетельством, зарегистрированным (переподчинённым) КУЦ РК, могут запросить регистрацию (переподчинение) нового регистрационного свидетельства, прибыв в КУЦ РК и предоставив:

- заявление на регистрацию (переподчинение) регистрационного свидетельства, аккредитованного УЦ;
- копию свидетельства об аккредитации УЦ;
- регистрационное свидетельство аккредитованного УЦ в форме электронного документа.

КУЦ РК осуществляет регистрацию (переподчинение) регистрационного свидетельства, подчинённого УЦ в течение 15 рабочих дней после подачи аккредитованным УЦ вышеперечисленных документов.

3.2.1. Способ доказательства обладания личным ключом

При запросе на выдачу регистрационного свидетельства КУЦ РК проверяет факт обладания закрытым ключом, соответствующим открытому ключу, на который запрашивается регистрационное свидетельство: при идентификации КУЦ РК проверяет корректность составления заявления и наличие необходимых документов, в том числе наличия свидетельства об аккредитации удостоверяющего центра.

3.2.2. Представление интересов заявителя третьим лицом

Документы подаются физическими лицами, представляющими интересы заявителя на основании доверенности установленной формы в соответствии с действующим законодательством Республики Казахстан. Доверенность должна быть нотариально заверена.

3.2.3. Проверка (идентификация) заявителя

Сведения, указанные в заявлении аккредитованного УЦ на регистрацию (переподчинение) регистрационного свидетельства, подтверждаются при личном прибытии представителя заявителя в КУЦ РК представлением следующих документов:

- заявление на регистрацию (переподчинение) регистрационного свидетельства, аккредитованного УЦ;
- копию свидетельства об аккредитации УЦ;
- регистрационное свидетельство аккредитованного УЦ в форме электронного документа.

3.2.4. Непроверяемая информация абонента

Не применимо.

3.2.5. Проверка полномочий

В процессе рассмотрения заявления на переподчинение регистрационного свидетельства аккредитованного УЦ, КУЦ РК действует в соответствии с пунктом 3.2.3. Дополнительных проверок таких полномочий не проводится, так как они подтверждаются соответствующим заявлением и свидетельством об аккредитации УЦ.

Вместе с тем, КУЦ РК оставляет за собой право в случаях, вызывающих сомнения при такой проверке, требовать от заявителя представления дополнительных документов, подтверждающих сведения, указанные в заявлении, а также официально направить запрос в МИК о подтверждении прохождения заявителя процедуры аккредитации УЦ.

3.2.6. Критерии взаимодействия

КУЦ РК и заявитель при необходимости для случаев ускоренного выпуска или отзыва регистрационного свидетельства могут заключить между собой соглашение о выдаче и отзыве регистрационного свидетельства.

3.3. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ЗАЯВИТЕЛЯ ПРИ ПОВТОРНОМ ВЫПУСКЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

КУЦ РК не допускает замену ключевых пар в действующих подчинённых регистрационных свидетельствах подчинённых УЦ. Для использования новых ключевых пар, подчинённому УЦ необходимо выпустить соответствующее регистрационное свидетельство и пройти процедуру регистрации (переподчинения) нового регистрационного свидетельства.

В случае необходимости регистрации (переподчинения) нового регистрационного свидетельства подчинённого УЦ до истечения срока существующего регистрационного свидетельства.

В случае регистрации (переподчинения) нового регистрационного свидетельства после отзыва существовавших подчинённых регистрационных свидетельств, подчинённый УЦ проходит идентификацию для заявлений в соответствии с процедурой, описанной в п. 3.2 выше.

3.3.1. Идентификация и аутентификация запросов при плановой замене ключей

В данном случае КУЦ РК проверяет факт владения подписчиком закрытым ключом в том же порядке, как это изложено в пункте 3.2.1.

3.3.2. Идентификация и аутентификация запросов на замену ключей в сертификате после отзыва

В данном случае КУЦ РК проверяет факт владения подписчиком закрытым ключом в том же порядке, как это изложено в пункте 3.2.1.

3.4. ПРОВЕРКА (ИДЕНТИФИКАЦИЯ) ПОДПИСЧИКА КУЦ РК ПРИ ОТЗЫВЕ ПОДЧИНЁННОГО РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

Заявление на отзыв подчинённого регистрационного свидетельства подчинённого УЦ подаётся в бумажной форме при личном прибытии представителя заявителя. Заявление должно соответствовать требованиям законодательства Республики Казахстан. КУЦ РК проверяет (идентифицирует) личность заявителя в соответствии с перечнями документов, приведёнными в пункте 3.4.2.

В случае успешной проверки (идентификации) личности заявителя и соответствия предоставленных документов, КУЦ отзывает регистрационное свидетельство подчинённого УЦ.

3.4.1. Представление интересов заявителя третьим лицом

Документы подаются физическими лицами, представляющими интересы заявителя (юридического лица) на основании доверенности установленной формы в соответствии с действующим законодательством Республики Казахстан. Доверенность должна быть нотариально заверена.

3.4.2. Проверка (идентификация) заявителя

Сведения, указанные в заявлении подчинённого УЦ на отзыв регистрационного свидетельства, подтверждаются при личном прибытии представителя заявителя в КУЦ РК представлением следующих документов:

- заявление на отзыв подчинённого регистрационного свидетельства, заверенное печатью юридического лица подчинённого УЦ;
- доверенность на представителя заявителя (юридического лица подчинённого УЦ) в соответствии с п. 3.4.1. выше; для первого руководителя юридического лица или лица, исполняющего его обязанности, вместо доверенности представляется справка с места работы либо заверенная печатью юридического лица подчинённого УЦ копия приказа (решения, протокола) о назначении на должность первого руководителя или лица, исполняющего его обязанности;
- оригиналы документов, удостоверяющих личность представителя заявителя (юридического лица подчинённого УЦ) в соответствии с п. 3.4.1. выше.

4. ОПЕРАЦИОННЫЕ ТРЕБОВАНИЯ К ЖИЗНЕННОМУ ЦИКЛУ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.1. ЗАЯВЛЕНИЕ НА РЕГИСТРАЦИЮ (ПЕРЕПОДЧИНЕНИЕ) РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.1.1. Лица, имеющие право подавать заявления на регистрацию (переподчинение) регистрационного свидетельства аккредитованного УЦ

УЦ могут подавать заявления на регистрацию (переподчинение) регистрационного свидетельства подчинённого УЦ или на переподчинение существующего регистрационного свидетельства УЦ только при соблюдении условия, что УЦ является аккредитованным УЦ в ИОК КУЦ РК.

4.1.2. Порядок регистрации и выдачи регистрационных свидетельств КУЦ РК

Все заявители должны пройти процесс регистрации в КУЦ РК, состоящий из следующих шагов:

- подача заявления на регистрацию (переподчинение) регистрационного свидетельства аккредитованного УЦ;
- идентификация и аутентификация для заявления в соответствии с п. 3.2 выше;
- предоставление регистрационного свидетельства подчинённого УЦ, запрашиваемого к регистрации (переподчинению).

После рассмотрения документов КУЦ РК производит регистрацию (переподчинение) регистрационного свидетельства подчинённого УЦ в форме электронного документа, а также его копии на бумажном носителе и регистрирует его в регистре регистрационных свидетельств.

4.1.3. Процедура генерации ключевой пары подчинённых УЦ

Заявители (аккредитованные УЦ) генерируют свои ключевые пары самостоятельно с соблюдением требований КУЦ РК:

- Для ключевых пар, выпущенных в соответствии с алгоритмом RSA:
  - длина закрытого ключа — 4096 бит;
  - длина открытого ключа — 4096 бит.
- Для ключевых пар, выпущенных в соответствии с алгоритмом ГОСТ 34.310-2004:
  - длина закрытого ключа — 256 бит;
  - длина открытого ключа — 512 бит.

4.2. ОБРАБОТКА ЗАЯВЛЕНИЯ НА РЕГИСТРАЦИЮ (ПЕРЕПОДЧИНЕНИЕ) РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.2.1. Аутентификации и идентификации заявки

Любая процедура идентификации и аутентификации при выпуске регистрационного свидетельства выполняется в том же порядке, что и первоначальная проверка идентичности, изложенная в разделе 3.2.

4.2.2. Подтверждение принадлежности и действительности открытого ключа ЭЦП

Подтверждение принадлежности и действительности открытого ключа ЭЦП производится в соответствии с положениями п. 3.2 выше.

4.2.3. Отказ в приёме заявления на регистрацию (переподчинение) регистрационных свидетельств аккредитованных УЦ

КУЦ РК отклоняет заявление на регистрацию (переподчинение) регистрационного свидетельства аккредитованного УЦ, если выполняется хотя бы одно из следующих условий:

- аккредитованный УЦ не предоставил необходимые документы;
- аккредитованный УЦ предоставил недостоверную информацию.

4.2.4. Срок рассмотрения заявлений на регистрацию (переподчинение) регистрационных свидетельств

КУЦ РК рассматривает заявления на выдачу (переподчинение) регистрационных свидетельств подчинённых УЦ в срок не более 15 календарных дней с момента получения всех необходимых данных.

Мотивированный ответ об отказе в регистрации (переподчинении) регистрационного свидетельства аккредитованного УЦ предоставляется в течение 15 рабочих дней с момента предоставления необходимых документов.

4.3. ВЫДАЧА (ПЕРЕПОДЧИНЕНИЕ) РЕГИСТРАЦИОННЫХ СВИДЕТЕЛЬСТВ ПОДЧИНЕННЫХ УЦ

4.3.1. Действия КУЦ РК в ходе регистрации (переподчинения) регистрационных свидетельств

Регистрационное свидетельство подчинённого УЦ регистрируется (переподчиняется) КУЦ РК на основании заявления. Процедура регистрации (переподчинения) регистрационного свидетельства требует идентификации подчинённого УЦ при личной явке представителя подчинённого УЦ в КУЦ РК.

КУЦ РК осуществляет регистрацию (переподчинение) регистрационного свидетельства подчинённого УЦ на основе информации, предоставленной в заявлении.

4.3.2. Уведомление подчинённых УЦ о регистрации (переподчинении) регистрационного свидетельства, подчинённого УЦ

Официальным уведомлением о факте регистрации (переподчинении) регистрационного свидетельства является опубликование данного свидетельства в регистре регистрационных свидетельств на Интернет-ресурсе КУЦ РК. При положительном результате обработки заявления на регистрацию (переподчинение) регистрационного свидетельства, заявитель получает в качестве ответа регистрационное свидетельство подчинённого УЦ, подписанное регистрационным свидетельством КУЦ РК.

КУЦ РК направляет извещение о регистрации (переподчинении) регистрационного свидетельства подчинённого УЦ заявителю средствами электронной почты. В случае если подчинённый УЦ не получил данного уведомления, КУЦ РК ответственности не несёт.

4.4. ПРИНЯТИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.4.1. Принятие регистрационного свидетельства КУЦ РК подчиненным УЦ

Следующая реакция подчинённого УЦ означает принятие им регистрационного свидетельства:

- отсутствие возражений со стороны подчинённого УЦ против принятия регистрационного свидетельства, подчинённого УЦ или его содержания;
- использование подчинённого регистрационного свидетельства.

4.4.2. Уведомление КУЦ РК других сторон о регистрации (переподчинении) регистрационных свидетельств подчинённых УЦ

КУЦ РК направляет уведомление подчинённому УЦ посредством электронной почты на адрес, указанный при подаче заявления.

КУЦ РК публикует информацию о выпуске нового подчинённого регистрационного свидетельства или переподчинении существующего регистрационного свидетельства на Интернет-ресурсе КУЦ РК в разделе «Новости», расположенном по адресу http://root.gov.kz/novosti.html.

4.4.3. Публикация регистрационного свидетельства удостоверяющим центром

КУЦ РК размещает выпущенные (переподчиненные) регистрационные свидетельства на Интернет-ресурсе КУЦ РК в разделе «Регистр регистрационных свидетельств», расположенному по адресу http://root.gov.kz/certificates.html.

4.5. ИСПОЛЬЗОВАНИЕ КЛЮЧЕВОЙ ПАРЫ И РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.5.1. Использование закрытых ключей и регистрационных свидетельств подчинёнными УЦ

Использовать закрытый ключ разрешается только после выполнения следующих действий:

- подчинённый УЦ принял требования настоящих Правил;

- КУЦ РК в порядке, установленном действующим законодательством Республики Казахстан, зарегистрировал (переподчинил) регистрационное свидетельство подчинённого УЦ для соответствующего открытого ключа.

Использование закрытого ключа означает принятие подчинённым УЦ Политики применения регистрационных свидетельств КУЦ РК и настоящих Правил.

Регистрационное свидетельство подчинённого УЦ должно использоваться только в соответствии с:

- действующим законодательством Республики Казахстан;
- Политикой применения регистрационных свидетельств КУЦ РК;
- настоящими Правилами.

Использование регистрационных свидетельств подчинённых УЦ должно соответствовать содержанию расширения «keyUsage».

Обязанностью подчинённых УЦ является защита закрытых ключей и активационных данных от несанкционированного доступа в соответствии с требованиями действующего законодательства Республики Казахстан. Подчинённые УЦ не имеют права использовать закрытые ключи с истекшим сроком действия или в случае отзыва соответствующего регистрационного свидетельства.

4.5.2. Использование открытых ключей и регистрационных свидетельств подчинённых УЦ доверяющими сторонами

Доверяющие стороны, участники СУЦ РК, должны принять обязательства доверяющей стороны, регламентированные в:

- действующем законодательстве Республики Казахстан;
- Политике применения регистрационных свидетельств КУЦ РК;
- настоящих Правилах.

Перед принятием решения о доверии к регистрационному свидетельству подчинённого УЦ, участники СУЦ РК должны выполнить следующие действия.

1. Проверить соответствующий электронный документ, подписанный регистрационным(-и) свидетельством(-ами) подчинённого УЦ.
2. Удостовериться в действительности регистрационного свидетельства подчинённого УЦ, выполнив следующие действия:
   а) определить полную цепочку регистрационных свидетельств вплоть до корневого регистрационного свидетельства КУЦ РК;
   б) оценить соответствие всех регистрационных свидетельств в цепочке следующим критериям:
      - сфера применения в соответствии с соответствующей политикой применения регистрационного свидетельства;
      - содержанию полей «keyUsage» и «extendedKeyUsage» регистрационного свидетельства;
   в) удостовериться, что все регистрационные свидетельства в цепочке подписаны КУЦ РК;
   г) удостовериться в действительности каждого регистрационного свидетельства на момент подписания документа.

4.6. ОБНОВЛЕНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

КУЦ РК не допускает изменения данных в регистрационном свидетельстве подчинённого УЦ, включая срок действия регистрационного свидетельства. В случае необходимости обновления данных регистрационного свидетельства подчинённому УЦ необходимо запросить регистрацию (переподчинение) нового действительного регистрационного свидетельства (см. п. 4.1 выше) и отозвать устаревшее регистрационное свидетельство (см. п. 4.6.1. ниже).

4.6.1. Основания обновления регистрационного свидетельства

Не применимо.

4.6.2. Кто может запросить обновление регистрационного свидетельства

Лица, имеющие право подавать заявления на обновление регистрационного свидетельства аккредитованного УЦ определены в пункте 4.1.1.

4.6.3. Обработка запросов на обновление регистрационного свидетельства

Порядок обработки запросов на обновление регистрационных свидетельств описан в пункте 4.1.2.

4.6.4. Уведомление пользователя о выдаче обновленного регистрационного свидетельства

Уведомление пользователя о выдаче обновленного регистрационного свидетельства описано в пункте 4.3.2.

4.6.5. Процедура приема обновленного регистрационного свидетельства

Не применимо

4.6.6. Публикация обновленного регистрационного свидетельства УЦ

КУЦ РК размещает выпущенные (переподчиненные) регистрационные свидетельства на Интернет-ресурсе КУЦ РК в разделе «Регистр регистрационных свидетельств», расположенному по адресу http://root.gov.kz/certificates.html.

4.6.7. Уведомление КУЦ РК о выдаче регистрационного свидетельства другим объектам

Не применимо.

4.7. ЗАМЕНА КЛЮЧЕЙ В РЕГИСТРАЦИОННОМ СВИДЕТЕЛЬСТВЕ

КУЦ РК не допускает замены ключей в регистрационном свидетельстве подчинённого УЦ, включая срок действия регистрационного свидетельства. В случае необходимости замены ключей подчинённому УЦ необходимо запросить регистрацию (переподчинение) нового действительного регистрационного свидетельства (см. п. 4.1 выше) и отозвать устаревшее регистрационное свидетельство (см. п. 4.6.1.).

4.7.1. Основания для замены ключей в регистрационном свидетельстве

Не применимо.

4.7.2. Лица, имеющие права запрашивать новый открытый ключ

Лица, имеющие право запрашивать новый открытый ключ определены в пункте 4.1.1.

4.7.3. Обработка запросов на замену ключей в регистрационном свидетельстве

Порядок обработки запросов на замену ключей в регистрационном свидетельстве описан в пункте 4.1.2.

4.7.4. Уведомление абонента о выдаче регистрационного свидетельства с замененными ключами

Уведомление пользователя о выдаче регистрационного свидетельства с замененными ключами описано в пункте 4.3.2.

4.7.5. Процедура приема регистрационного свидетельства с замененными ключами

Не применимо.

4.7.6. Публикация регистрационного свидетельства УЦ с замененными ключами

КУЦ РК размещает выпущенные (переподчиненные) регистрационные свидетельства на Интернет-ресурсе КУЦ РК в разделе «Регистр регистрационных свидетельств», расположенному по адресу http://root.gov.kz/certificates.html.

4.7.7. Уведомление УЦ о выдаче регистрационного свидетельства с замененными ключами другим объектам

Не применимо.

4.8. ИЗМЕНЕНИЕ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА

КУЦ РК не допускает изменения данных в регистрационном свидетельстве подчинённого УЦ, включая срок действия регистрационного свидетельства. В случае необходимости изменения данных регистрационного свидетельства подчинённому УЦ необходимо запросить регистрацию (переподчинение) нового действительного регистрационного свидетельства (см. п. 4.1 выше) и отозвать устаревшее регистрационное свидетельство (см. п. 4.6.1.).

4.8.1. Основания изменения регистрационного свидетельства

Не применимо.

4.8.2. Кто может запросить изменение регистрационного свидетельства

Лица, имеющие право подавать заявления на изменение регистрационного свидетельства аккредитованного УЦ определены в пункте 4.1.1.

4.8.3. Обработка запросов на изменение регистрационного свидетельства

Порядок обработки запросов на изменение регистрационных свидетельств описан в пункте 4.1.2.

4.8.4. Уведомление абонента о выдаче измененного регистрационного свидетельства

Уведомление пользователя о выдаче измененного регистрационного свидетельства описано в пункте 4.3.2.

4.8.5. Процедура приема измененного регистрационного свидетельства

Не применимо.

4.8.6. Публикация измененного регистрационного свидетельства УЦ

КУЦ РК размещает выпущенные (переподчиненные) регистрационные свидетельства на Интернет-ресурсе КУЦ РК в разделе «Регистр регистрационных свидетельств», расположенному по адресу http://root.gov.kz/certificates.html.

4.8.7. Уведомление УЦ о выдаче измененного регистрационного свидетельства другим объектам

Не применимо.

4.9. ОТЗЫВ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

4.9.1. Основания для отзыва регистрационных свидетельств подчинённых УЦ

КУЦ РК отзывает регистрационные свидетельства подчинённых УЦ до истечения срока действия в следующих случаях:

1) по требованию владельца регистрационного свидетельства либо его представителя;
2) установления факта предоставления недостоверных сведений при получении регистрационного свидетельства;
3) смерти владельца регистрационного свидетельства;

4) изменения фамилии, имени или отчества (если оно указано в документе, удостоверяющем личность) владельца регистрационного свидетельства;
5) смены наименования, реорганизации, ликвидации юридического лица-владельца регистрационного свидетельства;
6) предусмотренных соглашением между удостоверяющим центром и владельцем регистрационного свидетельства;
7) по вступившему в законную силу решению суда.

4.9.2. Лица, имеющие право подавать заявления на отзыв регистрационных свидетельств подчинённых УЦ

К лицам, имеющим право подавать заявления на отзыв регистрационных свидетельств подчинённых УЦ относятся:

- подчинённые УЦ;
- уполномоченные представители подчинённых УЦ.

4.9.3. Процедуры отзыва регистрационного свидетельства для всех участников ИОК КУЦ РК

Отзыв регистрационного свидетельства подчинённого УЦ осуществляется на основании официального письма от подчинённого УЦ на бумажном носителе с приложением документа, подтверждающего факт наступления одного из случаев, предусмотренных п. 4.7.1 выше.

После получения необходимых документов КУЦ РК осуществляет проверку документов в срок не позднее 2 рабочих дней, следующих за рабочим днём, в течение которого было подано заявление. В случае успешного рассмотрения заявления, КУЦ РК осуществляет отзыв регистрационного свидетельства, публикует информацию об отозванном регистрационном свидетельстве в СОРС и уведомляет подписчика посредством электронной почты. КУЦ РК не несёт ответственности за получение подписчиком уведомления об отзыве регистрационного свидетельства.

4.9.4. Срок подачи заявлений на отзыв регистрационного свидетельства подчинённого УЦ

Подчинённые УЦ осуществляет своевременную подачу заявлений на отзыв регистрационных свидетельств в порядке установленными настоящими Правилами.

4.9.5. Срок рассмотрения заявлений на отзыв регистрационного свидетельства подчинённого УЦ

В соответствии с процедурой, описанной в п. 4.9.3. выше.

4.9.6. Требования о проверке отзыва регистрационного свидетельства подчинённого УЦ для доверяющих сторон

Участники СУЦ РК должны проверять статус регистрационных свидетельств подчинённых УЦ перед принятием решения об использовании указанных регистрационных свидетельств, посредством проверки наличия регистрационного свидетельства подчинённого УЦ в действующем СОРС.

КУЦ РК предоставляет необходимые механизмы проверки статуса регистрационных свидетельств в соответствии с настоящими Правилами (см. п. 2.2 выше).

4.9.7. Частота выпуска СОРС подчинённых УЦ

СОРС выпускается и публикуется не реже, чем 1 раз в 35 суток.

4.9.8. Максимальная задержка СОРС подчинённых УЦ

СОРС подчинённых УЦ публикуются на Интернет-ресурсе КУЦ РК незамедлительно после генерации.

4.9.9. Требование по доступности СОРС

КУЦ РК обеспечивает непрерывную доступность СОРС в соответствии с настоящими Правилами (см. п. 2.2 выше).

4.9.10. Требования к проверке статуса отзыва в режиме онлайн

Не применимо.

4.9.11. Другие формы доступных уведомлений об отзыве

КУЦ РК размещает СОРС на Интернет-ресурсе КУЦ РК в разделе «Регистр регистрационных свидетельств», расположенному по адресу http://root.gov.kz/certificates.html.

4.9.12. Особые требования при замене скомпрометированной пары ключей

Подписчики КУЦ РК, извещаются о компрометации или подозрении в компрометации закрытых ключей КУЦ РК любыми целесообразными способами.

В случае обоснованного подозрения о компрометации закрытого ключа подписчик и владелец соответствующего регистрационного свидетельства обязаны немедленно отозвать регистрационное свидетельство.

Владелец регистрационного свидетельства, кроме того, обязан в случае компрометации закрытых ключей или увольнения работника, имевшего доступ к закрытым ключам, отозвать соответствующие к этим ключам регистрационные свидетельства и для их замены запросить выпуск новых регистрационных свидетельств.

4.9.13. Требования по уведомлению при компрометации ключей подписчика

Подписчики КУЦ РК при компрометации или подозрении в компрометации своих закрытых ключей в обязательном порядке в кратчайшие сроки должны известить КУЦ РК, любыми целесообразными способами.

4.9.14. Основания приостановки действия сертификата

Не применимо.

4.9.15. Кто может запросить приостановку действия сертификата

Не применимо.

4.9.16. Процедура запроса на приостановку действия сертификата

Не применимо.

4.9.17. Пределы периода приостановки действия сертификата

Не применимо.

4.10. СЛУЖБА ПРОВЕРКИ СТАТУСА РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННЫХ УЦ

4.10.1. Эксплуатационные характеристики

Информация о статусе регистрационных свидетельств подписчиков подчиненных УЦ должна быть доступна по адресам указанным на интернет - ресурсах подчиненных УЦ через службы СОРС и OCSP.

4.10.2. Режим работы сервиса

СОРС доступен непрерывно в режиме 24 часа в сутки, 7 дней в неделю.

4.10.3. Дополнительные особенности

Не оговариваются.

4.11. ОКОНЧАНИЕ ПОДПИСКИ

Регистрационное свидетельство подчинённого УЦ автоматически становится недействительным при истечении срока действия в соответствии с п. 6.3.2. ниже.

Подчинённые УЦ вправе отозвать свои регистрационные свидетельства до окончания срока его действия (см. п. 4.6.1. выше).

4.12. ДЕПОНИРОВАНИЕ И ВОССТАНОВЛЕНИЕ КЛЮЧЕВОЙ ПАРЫ

КУЦ РК не осуществляет депонирование и восстановление ключевых пар подчинённых УЦ.

4.12.1. Политика и практика депонирования и восстановления ключевой пары

Не применимо.

4.12.2. Политика и практика инкапсуляции и восстановления ключевой пары

Не применимо.

5. УПРАВЛЕНЧЕСКИЕ, ОПЕРАЦИОННЫЕ И ФИЗИЧЕСКИЕ КОНТРОЛИ АКТИВОВ КУЦ РК

5.1. КОНТРОЛЬ ФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ АКТИВОВ КУЦ РК

КУЦ РК обеспечивает физическую безопасность систем КУЦ РК в соответствии с действующим законодательством Республики Казахстан. Детальные политики и процедуры мер обеспечения физической безопасности содержат конфиденциальную информацию КУЦ РК и поэтому не публикуются.

«Не применимо.

Управленческие, операционные и физические контроли» настоящих Правил содержит общий обзор этих мер.

КУЦ РК обеспечивает физическую безопасность систем КУЦ РК посредством организационно-технических и административных мероприятий, направленных на:

обеспечение физической безопасности работников КУЦ РК;

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

обеспечения информационной безопасности КУЦ РК;

контроль эффективности физической безопасности КУЦ РК.

5.1.1. Место размещения активов КУЦ РК

В зданиях, в которых находятся места размещения информационных активов КУЦ РК, обеспечиваются следующие условия:

- обеспечение физической безопасности деятельности КУЦ РК (см. п. 0 выше);
- обеспечение резервных объектов для поддержания непрерывности деятельности КУЦ РК в случаях чрезвычайной ситуации.

5.1.2. Физический доступ к информационным активам КУЦ РК

Информационные активы КУЦ РК защищены минимум четырьмя последовательными уровнями физической безопасности, характеризующимися последовательно усиливающимися требованиями по физическому доступу на каждый следующий уровень в соответствии с:

- внутренними политиками КУЦ РК по организации физической безопасности и разделения полномочий;
- внутренними политиками организаций, обеспечивающих размещение систем КУЦ 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 КУЦ 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 КУЦ РК, а также посредством организационных мероприятий, гарантирующих работу с носителями данных исключительно в присутствии ответственных уполномоченных работников КУЦ РК.

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

Места размещения аппаратного обеспечения, поддерживающего работу информационных активов КУЦ 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 КУЦ 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. Подверженность водному воздействию

Места размещения аппаратного обеспечения систем КУЦ РК определены с учётом минимизации рисков наводнения, оползней, селей, ураганов и т.д.

5.1.5. Влияние природных стихий на места размещения аппаратного обеспечения КУЦ РК

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

5.1.6. Предотвращение и защита от пожаров мест размещения аппаратного обеспечения КУЦ РК

Места размещения аппаратного обеспечения информационных активов КУЦ РК обеспечивают эффективное предупреждение и борьбу с пожарами, вредными воздействиями возгорания и задымления в соответствии с действующими нормативными правовыми актами Республики Казахстан.

5.1.7. Хранение носителей информации КУЦ РК

Все носители информации КУЦ РК, данные, автоматические журналы, резервные копии хранятся с обеспечением физической безопасности в соответствии с:

- внутренними политиками КУЦ РК по организации физической и информационной безопасности, а также разделения полномочий;
- внутренними политиками организаций, обеспечивающих размещение носителей информации КУЦ РК;
- законодательством Республики Казахстан.
- КУЦ РК обеспечивает защиту носителей вышеперечисленной информации от:
- нарушения вышеперечисленных регламентов;
- повреждения;
- неавторизованного изменения информации;
- раскрытия конфиденциальной информации.

5.1.8. Утилизация носителей информации и аппаратного обеспечения КУЦ РК

КУЦ РК обеспечивает утилизацию носителей информации и аппаратного обеспечения в соответствии с:

- внутренними политиками КУЦ РК по организации физической и информационной безопасности, а также разделения полномочий;
- внутренними политиками организации, обеспечивающих размещение носителей информации и систем КУЦ РК;
- законодательством Республики Казахстан;
- технической документацией для носителей информации и аппаратного обеспечения.

Все носители, на которых когда-либо хранилась конфиденциальная информация, приводятся в состояние непригодности для чтения. КУЦ РК обеспечивает утилизацию носителей информации криптографического аппаратного обеспечения (см. п. 6.2.1. ниже).

5.1.9. Резервное копирование информации КУЦ РК

КУЦ РК осуществляет резервное копирование программного обеспечения систем КУЦ 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 КУЦ РК

5.2.1. Распределение ответственных ролей

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

- проверка информации из заявлений на регистрацию (переподчинение) регистрационных свидетельств аккредитованных УЦ;
- приём, отказ в приёме или иную обработку заявлений на регистрацию (переподчинение) регистрационных свидетельств аккредитованных УЦ;
- регистрация (переподчинение) или отзыв подчинённых регистрационных свидетельств.
- Ответственные роли включают, но не ограничиваются следующими функциями:
- обслуживание подчинённых УЦ;
- операции с криптографическим аппаратным обеспечением;
- управление и обеспечение информационной безопасности;
- управления и обеспечение физической безопасности;
- администрирование программного обеспечения систем КУЦ РК;
- обслуживание аппаратного обеспечения систем КУЦ РК;
- управление и обеспечение обслуживающей инфраструктуры КУЦ РК.

КУЦ РК обеспечивает соответствие работников всех ответственных ролей квалификационным требованиям (см. п. 5.2.3. ниже, а также п. 5.3.2. ниже).

5.2.2. Численность персонала, необходимого для отдельной задачи

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

В частности, задачи по управлению жизненным циклом регистрационных свидетельств подчинённых УЦ предполагают участие ответственных сотрудников КУЦ и представителей подчинённого УЦ. Также задачи по управлению ключевым материалом КУЦ РК, управлению доступом к системам КУЦ РК, управлению изменениями в системах КУЦ РК, резервным копированием систем КУЦ РК и т.д. предполагают участие не менее двух работников, относящихся к двум независимым подразделениям КУЦ РК или РГП «ГТС».

5.2.3. Идентификация и аутентификация ответственной роли

Для каждой роли КУЦ РК определены должностные инструкции и квалификационные требования. Для каждого из работников КУЦ РК перед приёмом на работу проверяется соответствие квалификационным требованиям (см. п. 5.3.2. ниже), а также проводится подтверждение личности кандидата и сбор прочих документов в соответствии с законодательством Республики Казахстан.

Служебная деятельность работников КУЦ РК в ответственных ролях возможна только в пределах физически защищённого периметра КУЦ РК (см. п. 5.1.2. выше). Доступ работников в защищённый периметр сопровождается подтверждением личности работников. Работа с информационными системами КУЦ РК также сопровождается подтверждением личности работников.

5.2.4. Функции КУЦ РК, требующие разделения обязанностей

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

- администрирование информационных систем КУЦ РК;
- разработка систем КУЦ РК;
- управление жизненным циклом подчинённых регистрационных свидетельств подчинённых УЦ.

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

5.3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РАБОТНИКОВ КУЦ РК

КУЦ РК обеспечивает безопасность работников КУЦ РК в соответствии с:

- внутренними политиками КУЦ РК по организации физической безопасности;
- внутренними политиками организаций, обеспечивающих размещение систем и работников КУЦ РК;
- законодательством Республики Казахстан.

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

5.3.1. Требования к опыту и квалификации работников КУЦ РК

КУЦ РК обеспечивает соответствие работников минимальным требованиям к опыту и квалификации в соответствии с:

- внутренними кадровыми политиками и должностными инструкциями КУЦ РК или РГП «ГТС»;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- законодательством Республики Казахстан.

Подтверждение соответствия требованиям к опыту и квалификации осуществляется предоставлением подтверждающих дипломов, сертификатов, рекомендаций и т.д., с сохранением копий Службе кадровой работы.

5.3.2. Процедуры проверки работников КУЦ РК

КУЦ РК обеспечивает проверку работников перед приёмом и в течение действия трудового договора в соответствии с:

- внутренними кадровыми политиками и должностными инструкциями КУЦ РК или РГП «ГТС»;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- законодательством Республики Казахстан.

Проверки включают, как минимум, документальное подтверждение следующих вопросов:

- соответствие требованиям к опыту и квалификации (см. п. 5.3.1. выше);
- предоставление необходимых справок и подтверждений в соответствии с законодательством

Республики Казахстан и ролью работника КУЦ РК.

5.3.3. Требования к повышению квалификации работников КУЦ РК

КУЦ РК обеспечивает повышению квалификации работников с целью компетентного и качественного выполнения служебных обязанностей. Повышение квалификации работников КУЦ РК 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. Требование повышения квалификации работников КУЦ РК

Периодичность мероприятий по повышению квалификации работников КУЦ РК определяется в соответствии с:

- потребностями в целях осуществления деятельности КУЦ РК;
- внутренними кадровыми политиками и должностными инструкциями, а также бюджетами повышению квалификации персонала РГП «ГТС»;
- законодательством Республики Казахстан.

5.3.5. Перемещения работников КУЦ РК по службе

Перемещения работников КУЦ РК по службе определяется в соответствии с:

- потребностями в целях осуществления деятельности КУЦ РК;
- внутренними кадровыми политиками, должностными инструкциями и планами КУЦ РК и РГП «ГТС»;
- законодательством Республики Казахстан.

Решения по перемещениям работников КУЦ РК утверждаются директором РГП «ГТС».

5.3.6. Ответственность работника РГП ГТС за несанкционированные действия

Работники КУЦ РК и РГП «ГТС» несут ответственность за соблюдение внутреннего распорядка в соответствии с:

- внутренними политиками и должностными инструкциями КУЦ РК и РГП «ГТС»;
- внутренними политиками организации, обеспечивающих работу систем КУЦ РК;
- законодательством Республики Казахстан.

При обнаружении несанкционированных действий или подозрении на совершение несанкционированных действий, лицо, обнаружившее нарушение, сообщает об этом в КУЦ РК. Ответственный работник КУЦ РК 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 соответствии с регламентом по управлению инцидентами КУЦ РК.

5.3.7. Требования к независимым сторонам

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

К участию в качестве независимых наблюдателей допускаются:

- уполномоченные органы, имеющие отношение к функционированию КУЦ РК, ИОК КУЦ РК или ИОК подчинённых УЦ (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 КУЦ РК, аудиторы WebTrust и т.д.).

5.3.8. Документация, раскрываемая работникам КУЦ РК и РГП «ГТС»

КУЦ РК обеспечивает работников РГП «ГТС» минимумом необходимых материалов в целях:

- обучения и повышению квалификации в соответствии с должностными инструкциями (см. п. 5.3.3. выше);
- выполнения должностных обязанностей.

Обеспечение материалами осуществляется в соответствии с:

- внутренними политиками и должностными инструкциями КУЦ РК и РГП «ГТС»;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- законодательством Республики Казахстан.

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

5.4.1. Типы журналируемых событий

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

События жизненного цикла ключей КУЦ РК и подчинённых УЦ подлежащие документированию:

1) передача на хранение ключевой пары;
2) восстановление ключевой пары;
3) выведение материалов ключевой пары из использования;
4) уничтожение ключевой пары;
5) идентификация стороны, авторизующей операции управления жизненным циклом ключевой пары;
6) идентификация лиц, имеющих доступ к материалам ключевой пары;
7) передача на содержание устройств или других средств хранения ключевой пары;
8) компрометация закрытого ключа;
9) резервное копирование ключевой пары;
10) архивирование ключевой пары.

События жизненного цикла ключей КУЦ РК и клиентов КУЦ РК, подлежащие журналированию:

1) выпуск ключевой пары;
2) использование ключевой пары.

События управления жизненным циклом криптографического аппаратного обеспечения, подлежащие документированию:

1) получение криптографического аппаратного обеспечения;
2) установка криптографического аппаратного обеспечения.

События передачи на хранение/получение с хранения криптографического аппаратного обеспечения, подлежащие документированию:

1) демонтаж криптографического аппаратного обеспечения;
2) обслуживание криптографического аппаратного обеспечения;
3) уничтожение криптографического аппаратного обеспечения;

События управления жизненным циклом криптографического аппаратного обеспечения, подлежащие документированию:

1) использование криптографического аппаратного обеспечения.

События управления жизненным циклом регистрационного свидетельства, подлежащие журналированию/документированию:

1) получение заявления на выпуск/обновление/отзыв/ регистрационного свидетельства;
2) выпуск регистрационного свидетельства;
3) распространение открытого ключа КУЦ РК;
4) отзыв регистрационного свидетельства;
5) генерация и выпуск списка отозванных регистрационных свидетельств;

События, связанные с безопасностью, подлежащие журналированию:

1) запись критичных файлов;
2) действия, предпринятые по отношению к важной информации;
3) изменение профилей безопасности;
4) использование механизмов идентификации и аутентификации;
5) сбои систем, включая программное и аппаратное обеспечение;
6) действия работников, работающих в доверенных ролях и администраторов;
7) доступ к системам КУЦ РК и их компонентам.

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

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

5.4.2. Частота анализа контрольных протоколов

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

5.4.3. Срок хранения журналов

КУЦ РК хранит журналы в течение как минимум 90 календарных дней, после чего журналы подлежат архивированию и сдаче в архив в соответствии с п. 5.5 ниже.

5.4.4. Защита журналов

КУЦ РК обеспечивает защиту журналов от несанкционированного просмотра, модификации и удаления. Защита журналов обеспечивается организационными и техническими мерами.

5.4.5. Резервное копирование журналов

КУЦ РК осуществляет резервное копирование журналов на ежеквартальной основе. Резервные копии хранятся в соответствии с:

внутренними политиками КУЦ РК и РГП «ГТС» по физической и информационной безопасности;
внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
требованиями законодательства Республики Казахстан.

5.4.6. Система сбора журналов

Не применимо.

5.4.7. Уведомление субъекта, вызвавшего событие

Не оговаривается.

5.4.8. Оценка уязвимостей

КУЦ РК осуществляет периодическую оценку уязвимостей, а также уязвимостей, выявленных в рамках работы системы внутренних контролей КУЦ РК в соответствии с:

1) внутренними политиками КУЦ РК и 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 КУЦ РК;
- требованиями законодательства Республики Казахстан.

5.5. АРХИВ ЗАПИСЕЙ

5.5.1. Типы архивируемых событий

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

1) журналы событий;
- действующие, отозванные и истёкшие регистрационные свидетельства подчинённых УЦ;
- действующие, отозванные и истёкшие регистрационные свидетельства КУЦ РК;
- заявления на регистрацию (переподчинение) и отзыв регистрационных свидетельств подчинённых УЦ;
- списки отозванных регистрационных свидетельств КУЦ РК и подчинённых УЦ.

5.5.2. Срок хранения архива

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

- внутренними политиками КУЦ РК и РГП «ГТС» для каждого вида данных;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- действующим законодательством Республики Казахстан.

5.5.3. Защита архива

КУЦ РК обеспечивает защиту архивных материалов в соответствии:

- внутренними политиками КУЦ РК и РГП «ГТС» для каждого вида данных;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- действующим законодательством Республики Казахстан.

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

5.5.4. Условия архивирования

Архивирование материалов осуществляется в соответствии с:

- внутренними политиками КУЦ РК и РГП «ГТС» для каждого вида данных;
- внутренними политиками организаций, обеспечивающих работу систем КУЦ РК;
- законодательством Республики Казахстан.

5.5.5. Порядок получения и проверки архивной информации

Доступ к архивным материалам ограничен в соответствии с п 5.5.3 настоящих Правил. Ответственные работники КУЦ РК осуществляют проверку архивной информации в соответствии с положениями п. 5.7.4. ниже.

5.6. ЗАМЕНА КЛЮЧЕЙ КУЦ РК

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

- прекращает использование старых ключевых пар и соответствующих им регистрационных свидетельств;
- генерирует новые ключевые пары и соответствующие корневые регистрационные свидетельства.

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

5.7. КОМПРОМЕТАЦИЯ И АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ КЛЮЧЕЙ КУЦ РК

5.7.1. Процедуры обработки происшествий и компрометации

КУЦ РК обеспечивает создание и безопасное хранение резервных копий следующих видов критических данных на случай чрезвычайных происшествий или компрометации:

- заявления на регистрацию (переподчинение) или отзыв регистрационных свидетельств;
- журналы событий;
- CORC;
- ключевые пары КУЦ РК.

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

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

5.7.2. Повреждения вычислительных, программных ресурсов и/или данных

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

5.7.3. Компрометация закрытого ключа КУЦ РК

КУЦ РК обеспечивает работу системы внутренних контролей, включающую мониторинг на предмет возможной компрометации закрытых ключей КУЦ РК. В случае обнаружения компрометации или наличия обоснованных подозрений в компрометации закрытых ключей КУЦ РК сотрудник КУЦ РК проводит необходимые меры в соответствии с Регламентом действий при компрометации закрытого ключа КУЦ РК.

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

5.7.4. Возможности непрерывной деятельности после происшествий

В КУЦ РК принят утверждённый и протестированный детальный План обеспечения непрерывности и восстановления деятельности Корневого удостоверяющего центра Республики Казахстан и Национального удостоверяющего центра Республики Казахстан (далее – План), нацеленный на смягчение последствий реализации угроз, в том числе катастроф природного характера. План регулярно рассматривается на предмет необходимости обновления в соответствии с внутренними процедурами оценки рисков КУЦ РК.

КУЦ РК обладает резервными объектами с целью обеспечения непрерывности служб и ключевых функций КУЦ РК.

Время необходимое для восстановления критичных сервисов КУЦ РК, при возникновении внешних и/или внутренних угроз способных в той или иной степени повлиять на работоспособность КУЦ РК:

- Целевое время для полного восстановления КУЦ РК (RTO) = 2 месяца 4 часа 25 минут 39 сек;
- Частичное время восстановления КУЦ РК (pRTO) = 2 часа 10 мин;
- Среднее время между сбоями = в зависимости от возникающей угрозы.

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

5.8. ПРЕКРАЩЕНИЕ ДЕЯТЕЛЬНОСТИ КУЦ РК

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

- уведомление с информацией о статусе КУЦ РК для сторон, которых касается прекращение, в том числе подчинённых УЦ и участников ИОК КУЦ РК;
- сохранение архивов КУЦ РК в соответствии с требованиями законодательства Республики Казахстан и соответствующей Политикой применения регистрационных свидетельств;
- продолжение сервисов поддержки подчинённых УЦ;
- продолжение сервиса проверки отзыва и выпуск CORC;
- отзыв действующих не отозванных регистрационных свидетельств подчинённых УЦ, при необходимости;
- выпуск заменяющих регистрационных свидетельств удостоверяющим центром-правопреемником;
- дальнейшее местонахождение закрытых ключей КУЦ РК и криптографических модулей, содержащих эти закрытые ключи;
    - положения, необходимые для передачи сервисов КУЦ РК его правопреемнику.

6. КОНТРОЛЬ ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ КУЦ РК

6.1. ВЫПУСК И УСТАНОВКА КЛЮЧЕВЫХ ПАР КУЦ РК

6.1.1. Генерация ключевой пары

Подчинённые УЦ генерируют свои ключевые пары самостоятельно, а также сами определяют политику в отношении генерации ключевых пар своих подписчиков.

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

Генерация ключевых пар КУЦ РК осуществляется исключительно в соответствии с утверждённым внутренним регламентом, при участии компетентных ответственных работников и при наблюдении независимой стороны. Церемония генерации ключевых пар КУЦ РК актируется соответствующим протоколом за подписью всех участников церемонии. Протоколы хранятся и архивируются в соответствии с требованиями действующего законодательства Республики Казахстан и внутренними регламентами КУЦ РК.

Процесс генерации ключевой пары защищен от выбросов электромагнетического излучения. Данное требование реализовывается за счет внешней физической защиты аппаратно-программного комплекса «Certex HSM» посредством сейфа безопасности Lampertz 9.3. Данный сейф защищает от выбросов электромагнетического излучения с внешней пропускную способностью не менее чем 70 децибел.

6.1.2. Доставка закрытого ключа подчинённого УЦ в КУЦ РК

Для переподчинения регистрационного свидетельства УЦ, закрытый ключ УЦ не требуется, в этой связи доставка закрытого ключа УЦ в КУЦ РК не осуществляется.

6.1.3. Доставка открытого ключа подчинённого УЦ в КУЦ РК

Открытый ключ подчинённого УЦ предоставляется в КУЦ РК в составе регистрационного свидетельства подчинённого УЦ при регистрации (переподчинении) регистрационного свидетельства подчинённого УЦ.

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 КУЦ РК обеспечивает организационно-технические меры по обеспечению целостности и достоверности открытого ключа КУЦ РК.

6.1.5. Цели использования ключа

В соответствии с подпунктом 1.4 настоящих Правил.

6.1.6. Размеры ключей

Ключевые пары подчинённых УЦ выпускаются в соответствии с алгоритмом RSA и имеют длину:
закрытый ключ — 4096 бит;
открытый ключ — 4096 бит.

Также КУЦ РК выпускает ключевые пары подчинённых УЦ в соответствии с алгоритмом ГОСТ 34.310-2004 и имеющие длину:
закрытый ключ — 256 бит;
открытый ключ — 512 бит.

6.1.7. Параметры создания открытого ключа

Параметры создания ключевой пары определены в пункте 6.1.1.

6.2. КОНТРОЛИ ЗАЩИТЫ ЗАКРЫТЫХ КЛЮЧЕЙ КУЦ РК И ПОДЧИНЁННЫХ УЦ, А ТАКЖЕ УПРАВЛЕНИЯ ЖИЗНЕННЫМ ЦИКЛОМ КРИПТОГРАФИЧЕСКОГО АППАРАТНОГО ОБЕСПЕЧЕНИЯ КУЦ РК

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

6.2.1. Стандарты и контроль криптографического аппаратного обеспечения

Криптографическое аппаратное обеспечение КУЦ 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 третьего уровня безопасности.

КУЦ 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 КУЦ РК. КУЦ 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 настоящих Правил и процедурными правилами в соответствии с пунктом 5.2 настоящих Правил.

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

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

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

Криптографические операции, проводимые вручную и требующие использования закрытых ключей КУЦ РК, осуществляются с использованием резервной копии закрытого ключа КУЦ РК, защищённого при помощи разделённого секрета. Для этого информация, необходимая для восстановления резервной копии закрытого ключа КУЦ РК («секрет») делятся на n частей. Для успешного восстановления резервной копии закрытого ключа КУЦ 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 КУЦ РК в соответствии с требованиями законодательства Казахстан и внутренней регламентной документацией КУЦ РК в соответствии с пунктом 6.4.1. ниже.

6.2.3. Депонирование закрытых ключей подчинённых УЦ

КУЦ РК не осуществляет депонирование закрытых ключей, подчинённых УЦ.

6.2.4. Резервное копирование закрытого ключа КУЦ РК

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

6.2.5. Архивирование закрытого ключа КУЦ РК

Архивирование закрытых ключей КУЦ РК с истекшим сроком действия регистрационного свидетельства.

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

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

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

6.2.7. Хранение закрытого ключа КУЦ РК в криптографическом модуле

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

Закрытые ключи подчинённых УЦ должны храниться в сертифицированных защищённых носителях, в соответствии с требованиями стандарта PKCS#11.

6.2.8. Способы активации закрытого ключа КУЦ РК

Закрытые ключи КУЦ РК перед использованием вручную активируются в соответствии с положениями, описанными в пункте 6.2.2 настоящих Правил.

6.2.9. Метод деактивации личного ключа

Деактивация закрытого ключа КУЦ РК не осуществляется в связи с его безопасным хранением на аппаратно-криптографическом модуле КУЦ РК.

6.2.10. Способ уничтожения закрытого ключа КУЦ РК и подчинённых

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

Уничтожение закрытых ключей, подчинённых УЦ является ответственностью подчинённых УЦ.

6.2.11. Оценка криптографических модулей КУЦ РК и подчинённых УЦ

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

6.3. ДРУГИЕ АСПЕКТЫ УПРАВЛЕНИЯ КЛЮЧЕВОЙ ПАРОЙ КУЦ РК

6.3.1. Архивирование открытых ключей

Все открытые ключи КУЦ РК и подчинённых УЦ, для которых КУЦ РК когда-либо регистрировал (переподчинял) регистрационные свидетельства, архивируются в составе соответствующих регистрационных свидетельств в соответствии с положениями пункта 5.5 вышенастоящих Правил.

6.3.2. Сроки действия регистрационных свидетельств и использования ключевых пар

Регистрационные свидетельства КУЦ РК генерируются со сроком действия не более чем в 10 лет. Регистрационные свидетельства подчинённых УЦ должны выпускаться со сроком действия в 5 лет. В случае отзыва регистрационных свидетельств КУЦ РК или подчинённых УЦ срок действия заканчивается на момент отзыва. Использование ключевых пар отозванных регистрационных свидетельств КУЦ РК или подчинённых УЦ не допускается.

6.4. АКТИВАЦИОННЫЕ ДАННЫЕ

6.4.1. Генерация и установка данных активации закрытых ключей

Генерация закрытых ключей КУЦ РК сопровождается созданием «секрета» на защищённых носителях ключевой информации в соответствии с процедурой, описанной в п. 6.2.2. выше. Использование «секрета» требует двухфакторной аутентификации — использования носителя части секрета и соответствующего уникального PIN-кода. Ответственные участники церемонии генерации закрытых ключей КУЦ 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.

6.4.2. Защита данных активации

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

6.4.3. Иные аспекты работы с данными активации

Данные активации закрытых ключей КУЦ 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 КУЦ 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. Требования к источнику точного времени

Для обеспечение высокой точности синхронизации системного времени все компоненты КУЦ РК, имеющие доступ к сети Интернет, сконфигурированы с сервером точного времени.

Все компоненты КУЦ РК, имеющие доступ к сети Интернет, установлены по универсальному скоординированному времени (UTC), работающие с поддержкой протоколов NTP для спутникового определения точного времени.

6.5.3. Оценка компьютерной безопасности

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

КУЦ 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

Порядок действий при разработке нового программного обеспечения КУЦ РК определен в Регламенте разработки программного обеспечения КУЦ РК.

6.6.2. Контроль управления безопасностью

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

6.6.3. Управление безопасностью жизненного цикла

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

6.7. КОНТРОЛИ БЕЗОПАСНОСТИ СЕТЕЙ

КУЦ РК обеспечивает безопасность внутренних сетей, а также безопасность данных, передаваемых по внешним сетям. КУЦ 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 КУЦ РК.

7. ПРОФИЛИ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ И СОРС

7.1. ПРОФИЛЬ РЕГИСТРАЦИОННОГО СВИДЕТЕЛЬСТВА ПОДЧИНЁННОГО УЦ

7.1.1. Профиль регистрационного свидетельства RSA для подчинённого УЦ

Поле	Описание	OID, критичность	Содержание
Базовые поля регистрационного свидетельства в формате X.509			
Version	Версия стандарта X.509	–	V3
SerialNumber	Серийный номер регистрационного свидетельства должен быть положительным, целым числом (20 байтов) и должен соответствовать требованиям п.4.1.2.2 стандарта RFC5280	–	–
SignatureAlgorithm	Алгоритм подписи	1.2.840.113549.1.1.11	sha256WithRSAEncryption
Subject	Данные Владельца 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	L = Subordinate CA's city (required) S = Subordinate CA's state (required) C = KZ (required) O = Legal name of organisation that possesses Subordinate CA (required) CN = Subordinate CA's name (required)
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	CN =2.5.4.3 O=2.5.4.10 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» C = KZ
PublicKey	Значение открытого ключа (4096 бит)	1.2.840.113549.1.1.1	–
Дополнительные поля регистрационного свидетельства в формате X.509			
Subject Key Identifier	Идентификатор ключа субъекта (4 байта). ID ключа на HSM	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа субъекта (4 байта). ID ключа на HSM	2.5.29.35	–
Basic Constraints	Основные ограничения	2.5.29.19, critical	Тип субъекта = ЦС; Ограничение на длину = Отсутствует
Key Usage	Использование ключа	2.5.29.15, critical	Подписание регистрационного свидетельства, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Ceritifcate Policy	Политика регистрационного	2.5.29.32	[1]Политика регистрационного свидетельства:

	свидетельства		Идентификатор политики = значение [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор:
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) Дополнительное имя: URL=http://root.gov.kz/cert/root_rsa.cer
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.root.gov.kz/rsa.crl URL=http://crl1.root.gov.kz/rsa.crl
Digital Signature	Цифровая подпись Центра сертификации (4096 бит)	1.2.840.113549.1.1.11	sha256WithRSAEncryption

7.1.2. Профиль регистрационного свидетельства ГОСТ для ЭЦП подчинённого УЦ

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 хэширования	1.2.398.3.10.1.3.1.1.0	Алгоритм хеширования ГОСТ 34.311-95
Subject	Данные владельца 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	L = Subordinate CA's city (required) S = Subordinate CA's state (required) C = KZ (required) O = Legal name of organisation that possesses Subordinate CA (required) CN = Subordinate CA's name (required)
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	CN =2.5.4.3 O=2.5.4.10 C=2.5.4.6	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) (обязательное поле) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» (обязательное поле)

			C = KZ(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 (4 байта). ID ключа на HSM	2.5.29.14	–
Authority Key Identifier	Идентификатор ключа центра сертификации (4 байта). ID ключа на HSM	2.5.29.35	–
Basic Constraints	Основные ограничения	2.5.29.19, critical	Тип субъекта = Центр сертификации; Ограничение на длину = Отсутствует
Key Usage	Использование ключа	2.5.29.15, critical	Подписание регистрационных свидетельств, Автономное подписание списка отзыва (CRL), Подписание списка отзыва (CRL)
Ceritifcate Policy	Политика регистрационного свидетельства	2.5.29.32	[1]Политика регистрационного свидетельства: Идентификатор политики=значение [1,1]Сведения квалификатора политики: Идентификатор квалификатора политики = CPS Квалификатор:
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 Дополнительное имя: URL=http://root.gov.kz/cert/root_gost.cer
Crl Distribution Points	2.5.29.31	Точки распространения списков отзыва	[1]Точка распределения списка отзыва (CRL) Имя точки распространения: Полное имя: URL=http://crl.root.gov.kz/gost.crl URL=http://crl1.root.gov.kz/gost.crl
Digital Signature	Цифровая подпись Центра сертификации (512 бит)	1.2.398.3.10.1.1.1.2	–

7.1.3. Профиль списка отозванных регистрационных свидетельств для ЭЦП в формате X.509

Название	Содержание
Version — Версия	V2
Issuer — Издатель СОРС	CN = НЕГІЗГІ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA) O = РМК «МЕМЛЕКЕТТІК ТЕХНИКАЛЫҚ ҚЫЗМЕТ» C=KZ
thisUpdate — Время издания СОРС	Valid from: YYMMDDHHMMSSZ
nextUpdate — Следующее обновление СОРС	Valid to: YYMMDDHHMMSSZ
signatureAlgorithm — Алгоритм подписи	sha256RSA

Основные ограничения по типу субъекта	Subject
Основные ограничения на длину пути	—

7.1.4. Обработка семантики критического расширения

Не применимо.

7.2. ПРОФИЛЬ OCSP

В КУЦ РК OCSP не используется.

7.2.1. Номер версии

Не применимо.

7.2.2. Расширения OCSP

Не применимо.

8. АУДИТ СООТВЕТСТВИЯ

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

Все подчинённые УЦ обязаны предоставлять в КУЦ РК не реже чем раз в год свидетельства успешной сертификации на соответствие требованиям международного стандарта WebTrust. Отсутствие своевременного подтверждения соответствия требованиям стандарта влечёт отзыв регистрационного свидетельства подчинённого УЦ.

8.1. ПЕРИОДИЧНОСТЬ ПРОВЕДЕНИЯ АУДИТА

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

8.2. АУДИТОРЫ И ИХ КВАЛИФИКАЦИЯ

Аудит внутренней контрольной среды КУЦ 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 КУЦ РК И АУДИТОРСКИМИ ОРГАНИЗАЦИЯМИ

Аудиторские компании, проверяющие внутреннюю контрольную среду КУЦ РК на соответствие требованиям международного стандарта WebTrust, являются независимыми от РГП «ГТС» и МИК РК.

8.4. ЗАДАЧИ АУДИТА

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

1) Раскрытие бизнес-практик КУЦ РК:
- управление политикой применения регистрационных свидетельств;
- управление инструкцией по применению регистрационных свидетельств.

Контроли среды КУЦ РК:
- управление информационной безопасностью;
- классификация активов и управление ими;
- безопасность персонала;
- управление физической безопасностью;
- управление деятельностью КУЦ РК;
- управление доступом;
- управление разработкой и поддержкой систем;
- управление непрерывностью бизнеса;
- мониторинг и управление соответствием требованиям;
- протоколирование.

Контроли жизненного цикла ключей КУЦ РК:
- генерация ключей КУЦ РК;
- хранение, резервное копирование и восстановление ключей КУЦ РК;
- распространение публичных ключей КУЦ РК;
- использование ключей КУЦ РК;
- архивирование и уничтожение ключей КУЦ РК;
- контроли компрометации ключей КУЦ РК;
- управление жизненным циклом СКЗИ КУЦ РК.

Контроли управления жизненным циклом регистрационных свидетельств подчинённых УЦ.

8.5. МЕРЫ, ПРЕДПРИНИМАЕМЫЕ ПРИ ВЫЯВЛЕНИИ НЕДОСТАТКОВ И НАРУШЕНИЙ

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

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

8.6. СООБЩЕНИЕ О РЕЗУЛЬТАТАХ

Сообщение о результатах аудита описано в разделе 8.5.

9. ПРАВОВАЯ ДЕЯТЕЛЬНОСТЬ

9.1. ОПЛАТА УСЛУГ

КУЦ РК не взимает платы за предоставление услуг по ИОК КУЦ РК, а именно:
- регистрация заявлений на переподчинение, приостановку и отзыв регистрационных свидетельств подчинённых УЦ;
- регистрация (переподчинение) регистрационных свидетельств подчинённых УЦ;
- отзыв регистрационных свидетельств подчинённых УЦ;
- публикация СОРС;
- подтверждение принадлежности, подлинности и действительности выпущенных регистрационных свидетельств по официальным обращениям участников ИОК КУЦ РК (см. п. 9.12 ниже).

9.1.1. Оплата за выдачу или обновление регистрационного свидетельства

Выдача регистрационных свидетельств осуществляется бесплатно.

9.1.2. Оплата за доступ к регистрационному свидетельству

КУЦ РК не взимает плату за доступ к регистрационному свидетельству.

9.1.3. Оплата за доступ к информации статуса регистрационного свидетельства

Доступ к информации о СОРС осуществляется на бесплатной основе.

9.1.4. Оплата за другие услуги

Не применимо.

9.1.5. Политика возмещения расходов

Не применимо.

9.2. ФИНАНСОВАЯ ОТВЕТСТВЕННОСТЬ

9.2.1. Страховое покрытие

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

9.2.2. Иная финансовая ответственность

Не применимо.

9.2.3. Сфера действия страхования и гарантии для конечных объектов

Не применимо.

9.3. КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ КУЦ РК

9.3.1. Конфиденциальная информация КУЦ РК

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

9.3.2. Информация вне пределов конфиденциальной информации

Участники КУЦ РК, признают, что регистрационные свидетельства, информация об их отзыве или иная информация о статусе регистрационного свидетельства, публичная часть регистра регистрационных свидетельств и содержащаяся в них информация не рассматривается в качестве конфиденциальной информации.

9.3.3. Ответственность по защите конфиденциальной информации КУЦ РК

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

9.4. КОНФИДЕНЦИАЛЬНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.4.1. Обеспечение конфиденциальности КУЦ РК персональных данных подчиненных УЦ

КУЦ РК обеспечивает защиту персональных данных в соответствии с действующим законодательством Республики Казахстан. КУЦ РК не разглашает информацию, идентифицирующую заявителей на регистрацию (переподчинение) регистрационных свидетельств аккредитованных УЦ. В случае прекращения деятельности КУЦ РК персональные данные подписчиков и заявителей передаются в УЦ преемник в соответствии с положениями, перечисленными в п. 5.8 выше.

9.4.2. Информация, рассматриваемая в качестве персональных данных

КУЦ РК рассматривает в качестве персональных данных любую информацию об аккредитованных УЦ, подчинённых УЦ и их подписчиках, не доступную из открытых источников и из содержания выпущенных регистрационных свидетельств в соответствии с действующим законодательством Республики Казахстан.

9.4.3. Информация, не рассматриваемая в качестве персональных данных

КУЦ РК не рассматривает в качестве персональных данных информацию, содержащуюся в регистрационных свидетельствах подчинённых УЦ и их подписчиков, а также иную информацию, подлежащую обязательному опубликованию в соответствии с действующим законодательством Республики Казахстан. Использование подчинёнными УЦ или их подписчиками регистрационных свидетельств означает принятие положений настоящего Регламента и согласие на публикацию данных, не рассматриваемых в качестве конфиденциальных.

9.4.4. Ответственность за защиту персональных данных подчиненных УЦ

Все работники КУЦ РК, работающие с персональными данными подписчиков, несут ответственность по защите вверенных им персональных данных подчинённых УЦ в соответствии с действующим законодательством Республики Казахстан.

9.4.5. Уведомление и согласие на использование персональных данных

Предоставление персональных данных в КУЦ РК означает согласие на использование этих персональных данных в целях предоставления услуг ЦР и КУЦ РК в соответствии с действующим законодательством Республики Казахстан.

9.4.6. Раскрытие персональных данных подчиненных УЦ правоохранительным и судебным органам

КУЦ РК предоставляет конфиденциальную информацию о персональных данных подчиненных УЦ в правоохранительные и судебные органы в соответствии с действующим законодательством Республики Казахстан.

9.4.7. Другие основания для раскрытия персональных данных подчиненных УЦ

Не применяются.

9.5. ПРАВА НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ

КУЦ РК оставляет за собой права интеллектуальной собственности на регистрационные свидетельства подчинённых УЦ, которые он регистрирует (переподчиняет), и на информацию об их статусе. При этом КУЦ РК не запрещает копирование и распространение регистрационных свидетельств, подчинённых УЦ на неисключительной безвозмездной основе, при соблюдении условий полноты копирования и использования регистрационных свидетельств в соответствии с условиями заключенных договоров с подчинёнными УЦ. КУЦ

РК также не запрещает использование информации о статусе регистрационных свидетельств подчинённых УЦ для выполнения функций доверяющей стороны.

Подчинённые УЦ признают право интеллектуальной собственности КУЦ РК на настоящие Правила и другую документацию КУЦ РК, регламентирующую деятельность КУЦ РК и подчинённых УЦ.

Подчинённые УЦ сохраняют все свои права на все торговые и тому подобные марки и имена, содержащиеся в заявлениях на регистрацию (переподчинение) регистрационных свидетельств и отличительные (DN-) имена в выпущенных регистрационных свидетельствах подчинённых УЦ.

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

9.6. ОБЯЗАННОСТИ

9.6.1. Обязанности КУЦ РК

КУЦ РК несет обязанность за:

1) создание ключей электронных цифровых подписей с принятием мер для защиты закрытых ключей электронной цифровой подписи от неправомерного доступа;

2) выдачу, регистрацию, отзыв, хранение регистрационных свидетельств, ведение регистра регистрационных свидетельств, выданных в установленном порядке;

2-1) для каждого типа регистрационного свидетельства утверждение правил применения регистрационного свидетельства;

3) осуществление учета действующих и отозванных регистрационных свидетельств;

4) подтверждение принадлежности и действительности открытого ключа электронной цифровой подписи, зарегистрированного удостоверяющим центром в порядке, установленном законодательством Республики Казахстан;

КУЦ РК обязан принимать все необходимые меры для предотвращения утери, модификации и подделки находящихся на хранении открытых ключей электронной цифровой подписи.

За неисполнение обязанности, предусмотренной пунктом выше, КУЦ РК несет ответственность в соответствии с действующим законодательством Республики Казахстан.

9.6.2. Обязанности ЦР

ЦР несет обязанность за:

- прием и проверку документов;
- идентификацию заявителя;
- выдача переподчиненного регистрационного свидетельства заявителю;
- хранение документов на выпуск регистрационных свидетельств заявителей.

9.6.3. Обязанности абонента

Владелец регистрационного свидетельства вправе требовать от удостоверяющего центра отзыва регистрационного свидетельства в случаях, если он предполагает нарушение режима доступа к закрытому ключу электронной цифровой подписи, соответствующему открытому ключу, указанному в регистрационном свидетельстве.

Владелец регистрационного свидетельства обязан:

1) предоставлять удостоверяющему центру достоверную информацию;

2) пользоваться закрытым ключом, соответствующим открытому ключу, указанному в регистрационном свидетельстве;

3) принимать меры для защиты принадлежащего ему закрытого ключа электронной цифровой подписи от неправомерного доступа и использования, а также хранить открытые ключи в порядке, установленном законодательством Республики Казахстан.

9.6.4. Обязанности доверяющих сторон

Не применимо

9.6.5. Обязанности других участников

Не применимо.

9.7. ОТЗЫВ ГАРАНТИЙ

Не применимо.

9.8. ОГРАНИЧЕНИЯ ОТВЕТСТВЕННОСТИ

Не применимо.

9.9. ГАРАНТИИ

9.9.1. Гарантии КУЦ РК

КУЦ РК гарантирует:

- отсутствие в выпущенных или переподчинённых регистрационных свидетельствах подчинённых УЦ умышленных искажений фактов, внесённых КУЦ РК или известных ему;
- отсутствие в информации регистрационных свидетельств КУЦ РК и подчинённых УЦ случайных ошибок, допущенных КУЦ РК вследствие халатности при рассмотрении заявлений на регистрацию (переподчинение) или при регистрации (переподчинении) регистрационных свидетельств;
- соответствие регистрационных свидетельств КУЦ РК и подчинённых УЦ требованиям законодательства Республики Казахстан, существенным требованиям соответствующей Политики применения регистрационных свидетельств и настоящих Правил;
- соответствие сервисов отзыва регистрационных свидетельств требованиям действующего законодательства Республики Казахстан, существенным требованиям соответствующей Политики применения регистрационных свидетельств и настоящих Правил во всех существенных аспектах.

Кроме того, КУЦ РК обязуется обеспечивать условия для выполнения гарантий и заверений подписчика и доверяющей стороны, изложенные в настоящих Правилах в п. 9.9.2. ниже и в п. 9.9.3. ниже.

9.9.2. Гарантии подчинённых УЦ

Подчинённые УЦ гарантируют выполнение следующих условий:

1) для каждой ЭЦП, сформированной с помощью закрытого ключа, который соответствует открытому ключу, указанному в регистрационном свидетельстве подчинённого УЦ, что:
   - данная ЭЦП принадлежит подчинённому УЦ;
   - соответствующее регистрационное свидетельство было принято подписчиком;
   - соответствующее регистрационное свидетельство не просрочено, не отозвано и его действие не приостановлено на момент формирования ЭЦП;
   - их закрытые ключи защищены, и к ним никогда не имело доступа ни одно неуполномоченное лицо;
   - все сведения, представленные подчинённым УЦ для заявления на регистрацию (переподчинение) регистрационного свидетельства, достоверны;
   - вся информация, содержащаяся в регистрационном свидетельстве подчинённого УЦ, достоверна;
   - регистрационное свидетельство используется в соответствии с:
     - действующим законодательством Республики Казахстан;
     - существенными требованиями Политики применения регистрационных свидетельств КУЦ РК;
     - существенными требованиями настоящих Правил;
   - подписчики подчинённого УЦ не являются удостоверяющими центрами и не используют закрытые ключи, которые соответствуют открытым ключам, указанным в регистрационных свидетельствах, в целях электронной цифровой подписи каких-либо регистрационных свидетельств (или любого другого формата удостоверений открытого ключа) или списков отозванных регистрационных свидетельств.

Кроме того, подчинённый УЦ обязан выполнять условия гарантий и заверений доверяющей стороны, изложенные в настоящих Правилах в п. 9.9.3. ниже.

9.9.3. Гарантии доверяющих сторон

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

9.10. СРОК ДЕЙСТВИЯ И ПОРЯДОК ПРЕКРАЩЕНИЯ ДЕЙСТВИЯ

9.10.1. Вступление в силу

Настоящие Правила вступают в силу незамедлительно с момента опубликования на Интернет-ресурсе КУЦ РК.

9.10.2. Прекращение действия

Настоящие Правила остаются в силе до замены новой версией в течение функционирования КУЦ РК. Замена новой версией осуществляется в соответствии с п. 1.6 выше.

9.10.3. Правовые последствия прекращения действия

С момента прекращения действия настоящих Правил подчинённые УЦ и участники СУЦ РК остаются связанными условиями последней версии Правил по всем регистрационным свидетельствам до момента истечения периода действия каждого из регистрационных свидетельств.

9.11. ИНДИВИДУАЛЬНЫЕ УВЕДОМЛЕНИЯ И ВЗАИМОДЕЙСТВИЕ С УЧАСТНИКАМИ

КУЦ РК использует любые доступные методы официального уведомления участников ИОК КУЦ РК, подчинённых УЦ и участников ИОК подчинённых УЦ.

Вопросы взаимодействия участников ИОК КУЦ РК друг с другом не регламентируются.

9.12. ПОПРАВКИ

9.12.1. Внесение поправок

Изменения и дополнения в Правила готовится службой инфраструктуры открытых ключей и оформляются в виде отдельного документа, содержащего либо актуальный текст Правил, либо уведомление об изменениях и дополнениях в его актуальный текст.

Публикация актуальной редакции Правил или уведомления об изменениях и дополнений к ней осуществляется на официальном Интернет-ресурсе КУЦ РК по адресу: http://root.gov.kz.

9.12.2. Механизм и период уведомления

КУЦ РК оставляет за собой право без предварительного уведомления вносить несущественные изменения и дополнения в настоящие Правила, включая, но не ограничиваясь исправлением опечаток, изменением адресов, ссылок и контактной информации. Решения о том, являются ли данные изменения и дополнения существенными или нет, принимаются по исключительному усмотрению КУЦ РК.

9.12.3. Основания, при которых объектный идентификатор должен быть изменен

Если в связи с внесением изменений и дополнений в настоящие Правила определил необходимость изменения объектных идентификаторов в соответствующей Политике применения регистрационных свидетельств, новые объектные идентификаторы для каждого типа регистрационного свидетельства должны быть указаны в актуальном тексте данных Правил, которые должны быть введены в действие одновременно с изменениями и дополнениями в настоящие Правила.

9.13. 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.

9.14. ДЕЙСТВУЮЩЕЕ ЗАКОНОДАТЕЛЬСТВО

Юридическая сила, толкование данных Правил осуществляется в соответствии с действующим законодательством Республики Казахстан.

9.15. СООТВЕТСВИЕ ДЕЙСТВУЮЩЕМУ ЗАКОНОДАТЕЛЬСТВУ

Юридическая сила, толкование данных Правил осуществляется в соответствии с действующим законодательством Республики Казахстан.

9.16. ПРОЧИЕ ПОСТАНОВЛЕНИЯ

9.16.1. Полнота соглашения

Не оговаривается.

9.16.2. Передача прав

Не применимо.

9.16.3. Делимость

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

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

Не оговаривается.

9.16.5. Форс-мажор

Не оговаривается.

9.17. ДРУГИЕ ПОЛОЖЕНИЯ

Не оговаривается.